Some Fascinating Applications of the Theory of Groups

Saurabh Singal
October 31, 2004

Introduction

A group is a set with an associated binary operation satisfying certain mathematical properties. This simple algebraic structure has very rich applications because the elements of the set need not be just numbers – they can be matrices, planes, translations, rotations, reflections, in fact functions or operations of any kind.

Group theory has been applied in field as diverse as crystallography and game theory (See *Mathematical Ways for your Winning Plays by John H. Conway, Elwyn Berlekamp and Richard Guy*). In crystallography and in quantum mechanics, Groups serve as the natural language to describe the arrangement of molecules and the behaviour of particles. A striking example is the discovery of the *Ω-baryon*, an elementary particle belonging to a family of ten particles. It was the last member to be discovered. After the first nine members were discovered and their behaviour was modelled using group theory, it was thought there should be another particle in the family. This in turn lead to a search and the Ω-baryon was discovered in 1964. It was like someone telling you there is a gold coin in your pocket; you are unaware of its existence but when you put your hand in the pocket, you find it there, as if by magic.

We first define a group, present some simple illustrations and then describe some areas where groups have been applied.

A group *G* is a finite or infinite set together with a binary operation or composition that satisfies the four fundamental properties of closure, associativity, the identity property, and the inverse property. The operation with respect to which a group is defined is often called the "group operation," and a set is said to be a group "under" this operation if the following four properties are satisfied

1. *Closure*: If *a* and b are two elements in *G*, then the product $a \times b$ is also in *G*.

2. *Associativity*: The defined operation is associative, i.e., for all *a, b, c* in *G*,
$$(a \times b) \times c = a \times (b \times c) .$$

3. *Existence of Identity*: There is an identity element, often denoted by *e*, such that
$$e \times a = a \times e = a \text{ for all } a \text{ belonging to } G.$$

4. *Existence of Inverse*: Each element must have an inverse, that is for each element *a* in *G*, there must exist an element *b* in *G* such that $a \times b = b \times a = e$.

The number of elements in the set is called the order of the group. If the set is infinite, the group is called an infinite group

Examples.

Consider the set $S = \{0, 1\}$ and the composition *addition modulo 2* denoted by $\oplus_2$ .Then it can be verified that $(S, \oplus_2)$ forms a group since $1 \oplus_2 1 = 0$; $1 \oplus_2 0 = 1$, $0 \oplus_2 1 = 1$, and $0 \oplus_2 0 = 0$, and the first property (closure) is satisfied. Addition Modulo 2 is associative over real numbers. The identity element is 0. The inverse of 1 is 1; 0 is the inverse of 0.

$\oplus_2$	**0**	**1**
0	0	1
1	1	0

Table 1: Composition Table for the Group $(S, \oplus_2)$.

As a second example, consider the set $S = \{-1, 1\}$, the set of square roots of 1 and the operation multiplication. This forms a group of order 2. The identity element is 1. Both 1 and –1 are their own inverses, since 1×1 = identity element =1, as also $-1 \times -1 = 1$ = identity element. The composition table is given in Table 2. This group is denoted as C_2 and is called the cyclic group of order 2.

$\times$	**–1**	**1**
–1	1	–1
1	–1	1

Table 2: C_2, *, the Cyclic Group of Order 2 (Multiplication over The Square Roots of 1)*

There are two striking things about the simple examples presented.

First, this group is what is called a ***cyclic group***, that is, it can be generated by the powers of a single element, in this case –1, since $(-1)^2 = 1$ and of course $(-1)^1 = -1$. A cyclic group is usually denoted by $\boldsymbol{C_n}$. The cube roots of unity also form a group under multiplication as do the fourth roots of unity *{1,–1, i,–i}*. The composition table for this group is given in Appendix 1.

Secondly, the composition tables show that the structure of the two groups is the same. They are equivalent, or in technical terms, they are isomorphic. This property is very useful because if we know the properties of one group and a second group is isomorphic

to the first, then we know all the properties of the second group as well. And it turns out for small orders, that there are not too many distinct groups. For example, all groups of order 2 (having two elements) are isomorphic (or equivalent in a mathematical sense) to $\boldsymbol{C_2}$. All groups of order 6 are isomorphic to either the dihedral group $\boldsymbol{D_3}$ (symmetries of an equilateral triangle, described in Appendix 2) or the group $\boldsymbol{C_6}$ (the group formed by the sixth roots of unity under the operation multiplication)

The groups of symmetries of the five regular polyhedra provide beautiful examples of finite groups. Consider for example, the group of rotations of the cube.

The group formed by the rotations of a cube has 24 elements.

1. Rotations about the 3 axes of symmetry through the centres of the faces yield 9 elements, 3 elements each from rotation by 90^{o}, 180^{o}, and 270^{o} about each axis.
2. Rotations about the 4 axes through opposite pairs of vertices yield 2 elements each, for a total of 8 elements.
3. Rotations about the 6 axes through the midpoints of opposite pairs of edges yield 1 element each.

Therefore there are $3 \times 3 + 4 \times 2 + 6 \times 1 = 23$ elements, and when we include the identity element of no rotation, we get 24 elements.

Another way of looking at this group is to consider the permutations which take the four diagonals into one another, thus producing 4! =24 elements.

KNOTS, BRAIDS AND GROUPS

The mathematical theory of knots has its origins in William Thompson (later Lord Kelvin) postulating that matter consisted of atoms tied up in knots. The type of the knot would determine the physical and chemical properties of the element. This theory died out after Mendeleev published his Periodic Table of Elements.

For his purposes Lord Kelvin needed to see which different types of knots are possible, but to classify the types of knots one needed to precisely define the equivalence of knots, or more importantly, to define a knot. That was how mathematical theory of knots was born. In mathematics, a knot is defined as a *closed*, *non-self-intersecting curve* that is embedded in three dimensions and cannot be untangled to produce a simple loop (i.e., the unknot).

Closely related to knots are braids and links - a braid is an intertwining of some number of strings attached to top and bottom "bars" such that each string never "turns back up". Groups have been used to analyse knots and braids.

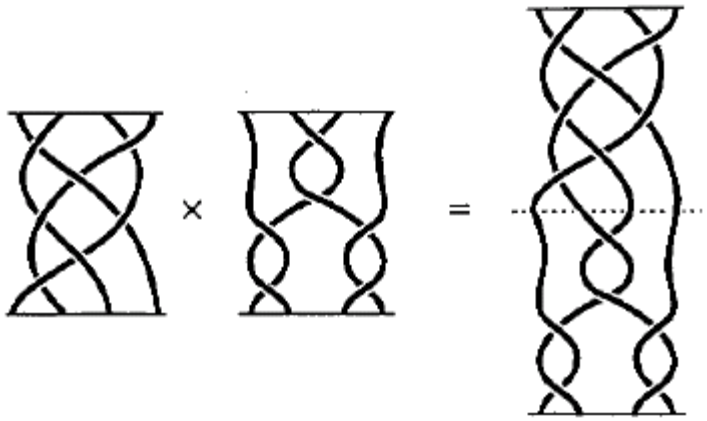

Figure 1: Composition of Two Braids

The Braid Group: First, we define the composition 'products of braids'. This is simply taking two braids and placing them end to end by joining the lower part of one braid to the upper part of the second braid, as shown in Figure 1. Let us consider all braids of n strands, n being any positive integer. The unit braid, e, is the *trivial braid* whose strands hang vertically without crossing. The product of this unit braid with another braid, i.e., appending it to any other braid does not change the other braid. For each braid b, there is an inverse braid b^{-1}, such that $b.b^{-1} = e$ .The inverse braid is the braid obtained by taking the horizontal mirror image of the given braid. This causes each crossing to cancel with its mirror image, resulting in all crossings dissolving. This is shown in Figure 2. (Figures 1 and 2 are from the book *Knots: Mathematics with a Twist* by *A. Sossinsky*). The braid composition is also associative and composition of two braids is another braid. Hence we get the braid group $\boldsymbol{B_n}$.

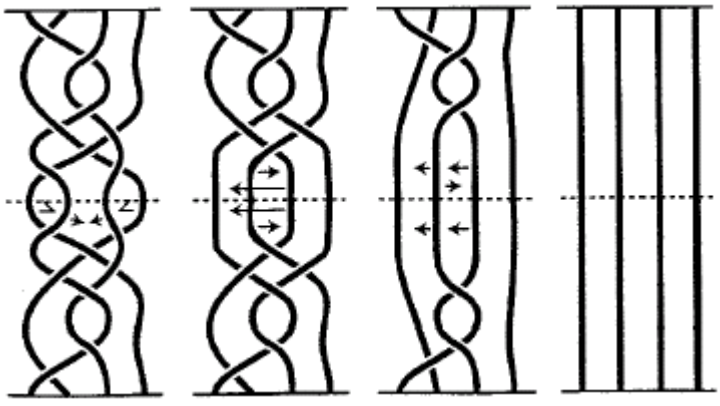

Figure 2: How Two Braids Cancel.

By being able to use the algebraic structure *group*, the mathematician Emil Artin was able to replace the geometry of braids to an algebraic structure. This led to systemization of the study of braids and allowed easy comparisons to see if two braids were equivalent.

INFORMATION THEORY

Claude Shannon in his seminal 1948 paper on Information Theory, "*A Mathematical Theory of Communication*" first described an error-correcting code and attributed it to Hamming.

As a simplistic illustration, consider the case where there are words consisting of 2 message bits. There can be a maximum of $2^2 = 4$ code words, since each message bit can be either 1 or 0. These may be represented by the vertices of the unit square in the plane. The words at the ends of an edge differ in one bit and those at the ends of diagonals differ from each other in two bits. We append a third bit, called the *parity bit*, which is 1 if there is an odd number of 1's in the message bits, and it is 0 if there is an even number of bits in the message bits. Thus 10 becomes 101 and 11 become 110. The 3-bit message has *even parity*. A single error in the transmission of the 3-bit codeword changes the parity to odd, which leads to error detection (though not error correction).

The *Hamming distance* between any two code words is defined as the number of co-ordinates or bits where the two words differ. Suppose that instead of the eight possible words of length 3, we discard four of them and retain only the following four: 000, 101, 011, and 110. Notice that the

- The Hamming distance between any two of the retained words is 2
- These are situated at the ends of the diagonals of the face of a unit cube illustrated in Figure 3.
- Their co-ordinates have even parity

A single error in the transmission of a word changes it to another word with Hamming distance 1 from the transmitted word.

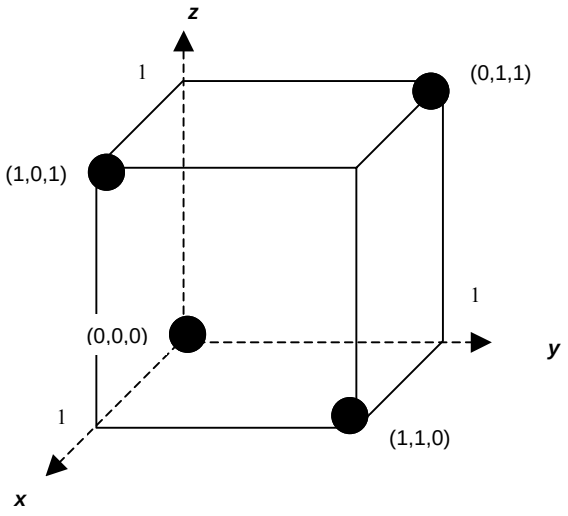

Figure 3: Code of Hamming Distance =2.

This is the reason why single errors can be detected. Notice that each of the code words differs from any other in two places; they have a *Hamming Distance* of 2. If one could travel only along the sides of the unit cube, this would be the shortest distance one would have to travel from one admissible codeword to another.

The concept of Hamming distance is useful in detecting and correcting errors. The minimum distance of a code is the least of the distances between all pairs of words in the code. The following results hold good:

1. A code can detect all combinations of m or fewer errors if and only if the minimum distance of the code is at least $m + 1$.
2. A code can correct all combinations of m or fewer errors if and only if the minimum distance of the code is at least $2m + 1$.

We could detect a single error ($m = 1$) in the above example because the minimum distance was 2. By using more parity bits so that we get a Hamming code of distance at least 3 ($2m + 1$ for $m = 1$), we would be able to correct single errors in the example given above.

The (n, r) Hamming code, contains r message bits and $(n - r)$ check bits, and is a subgroup of the group of all binary n-tuples under vector addition modulo 2. To see this, consider the set $\boldsymbol{B} = \{1, 0\}$ and the operation *addition modulo 2*. We have seen this illustration in the Introduction. Then $\boldsymbol{B}^n$ = all words of length n formed by elements of $\boldsymbol{B}$. One can verify that if u and v are in $\boldsymbol{B}^n$ so is $u \oplus_2 v$, each element is its own inverse, addition modulo 2 is associative and the identity element is the word with all zeros.

SPHERE PACKING

It is quite common that mathematicians develop abstract mathematics and their abstractions find industrial or technological application only much later on. The use of prime numbers and groups in cryptography is one such example. But at times, concreteness gives rise to abstractions. For example, Fourier developed *Fourier transform*, a technique to express a periodic function as an infinite sum (or definite integral) of relatively simpler functions *sin nx* and *cos nx*. Using this transform whenever it could be made to work, physicists transformed the classical physics. Mathematicians, on the other hand examined the reasons why it could not be made to work in all cases, and to their utmost surprise, they constructed the theory of infinite sets of Cantor. They had discovered the atom of the world of mathematics. Now everything was described in terms of sets elegantly. Such is the interplay between the concrete and the abstract. This interplay is visible in the case of sphere packing theory.

But first, what is sphere packing? The area of study called Sphere Packing started with attempts to prove (or disprove) *Kepler's conjecture*, which states, "No packing of balls of equal radius in three dimensions has density greater than the face centred cubic packing."

Starting with the bottom layer, the *Face Centred Cubic* packing is constructed by setting one layer of balls upon the others. The packing density, or the fraction of the space filled, is $\pi/\sqrt{18} = 0.74$ approximately. In two dimensions, Kepler's conjecture seeks the densest packing of unit disks in a plane. If we inscribe a disk in each hexagon of a regular hexagonal tiling of the plane, the optimal packing is produced and the density is $\pi/\sqrt{12} = 0.91$ approximately

In 1998, Thomas Hales, a mathematician at the University of Pittsburgh, announced that he had a proof of the Kepler conjecture.

There might not seem to be any connection between codes and sphere packing but John Leech used results in a generalised Hamming Code (called Golay code) to discover a packing in the 24 dimensional space that was more efficient than any other packing. (*Sphere Packings, Lattices and Groups by John H. Conway and N.J.A. Sloane*)

Related to the sphere packing is the study of minimal surfaces. What is the most efficient partition of the plane into regions of equal area such that the perimeter of the enclosing regions is minimised? The honeycomb conjecture asserts that the answer is the regular hexagonal tiling, also called honeycomb tiling. The three dimensional version of the problem is: how can space be divided into polyhedral cells of equal volume so as to minimize the surface area of the boundary? For a long time it was believed that the bee's honeycomb would provide the answer. The honeycomb is a six-sided prism. Three rhombi seal one end of the prism. But in 1964, L.Fejes Toth discovered that the obvious, elegant answer provided by Nature was incorrect. He provided an example of a cell that is more optimal than the three-dimensional honeycomb cell. Soap films and bubbles also provide many intriguing problems in this field many of which are still unsolved. Because of surface tension, soap bubbles try to minimize area for the volume they enclose, and are spherical. But when bubbles come together to form foam, they have polygonal faces. The first Fields Medal was awarded to Jesse Douglas for his work in the area of minimal areas related to soap films and bubbles.

CARD SHUFFLING

A perfect shuffle is one in which the deck is cut precisely in two equal parts and cards are interleaved. Example: if these cards are 1, 2 ...52, then two halves are 1, 2... 26 and 27, 28 ...52. After a perfect shuffle the order of the cards is either 1, 27, 2, 28... 26, 52 or 27,1, 28, 2,.....,52,26. Eight perfect shuffles restore a deck of 52 cards to the original order.

Group theorists have studied generalisation of shuffles on decks of arbitrary number of cards in detail. (*Magic Tricks, Card Shuffling and Computer Memories by S. Brent Morris*) In addition to their use in designing many card tricks, the group theoretic results from studying shuffles have been used to designing dynamic RAM and also in algorithms for shuffling tasks in parallel computers with multiple processors.

RUBIK'S CUBE AND OTHER GAMES

In the Rubik's cube, the cube is formed of 27 small cubes. Each face consists of 9 small squares, which we may call *facets*. Since a cube has 6 faces, we have 54 facets in all. Each facet is coloured with one of six different colours, there being exactly nine facets of each colour. The facets can be moved into different positions by various rotations. The problem consists of applying suitable rotations so that each of the six faces has all the nine facets of one colour.

Let us consider the rotations. Think of the cube as consisting of three vertical slices consisting of nine small cubes each The left vertical slice can be rotated about its horizontal axis of symmetry in the clockwise sense through an angle of 90^o, 180^o, 270^o, or 360^o (same as no rotation). This moves the facet in the top left corner into four different positions. Similarly, if we consider the rotations of the other two faces meeting at the top left vertex, the facet in the top left position can be moved to other corner positions. In all, the facet can take eight different positions. This is true of all the 54 facets. In all we have three non-zero rotations for each of the left, middle, right vertical faces, front, middle and back vertical faces, and bottom, middle and top horizontal faces, giving 27 basic rotations. Adding to these 27 rotations the identity or zero rotation, we get 28 rotations. These 28 rotations generate a group of very large order that is called the Rubik's Cube. The Rubik's group is a subgroup of the group that has all the different 28! permutations of the 28 rotations.

It is possible to 'solve' the Rubik cube without knowledge of groups. But the fast algorithms, which solve a cube from any initial position in 20 moves or less use group theory. A well known book on solving the Rubik's cube is *Rubik's Cubic Compendium by Erno Rubik, Tamas Varga, Gerzson Keri, Gyorgy Marx and Tamas Vekerdy*; and another one is *Notes on Rubik's Magic Cube by David Singmaster*. The more recent *Adventures in Group Theory: Rubik's Cube, Merlin's Machine and Other Mathematical Toys by David Joyner* has a description of many puzzles, their solving strategies and the underlying group theoretic framework.

QUESTIONS FOR MARKET PHILOSOPHERS.

Since Knots, Information Theory, and Shuffling are all helpful in thinking about the markets, and Group Theory is useful in studying all of these,

- Is it possible that Groups might help us in studying the markets?
- What symmetries of the markets groups might model?
- Can groups model the inherent shuffling mechanism of the market?
- Are there other examples where the obvious, beautiful and elegant design of nature is not optimal?
- Is there an analogue of surface tension in the markets? What perimeters, surfaces and volumes does the market try to optimise?

Appendix 1: The Cyclic Group C_4

Let S be the set of the fourth roots of unity, i.e., $S = \{1, -1, i, -i\}$. The table below gives a composition table for the operation of multiplication on elements of the S. We can verify that closure is satisfied, and we know that multiplication is associative. The element 1 is the identity and it can be seen that the inverse of 1 is 1, the inverse of 1 is -1, and i and $-i$ are the inverses of each other. Hence (S,*) is a group. Moreover the elements I is a generator of the group *since* $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

×	**1**	**–1**	**i**	**–i**
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	–i	–1	1
–i	–i	i	1	–1

Table 3: Cyclic Group C_4, Formed by Multiplication over the Fourth Roots of Unity.

Appendix 2: Dihedral Group D_3(Symmetries of an Equilateral Triangle)

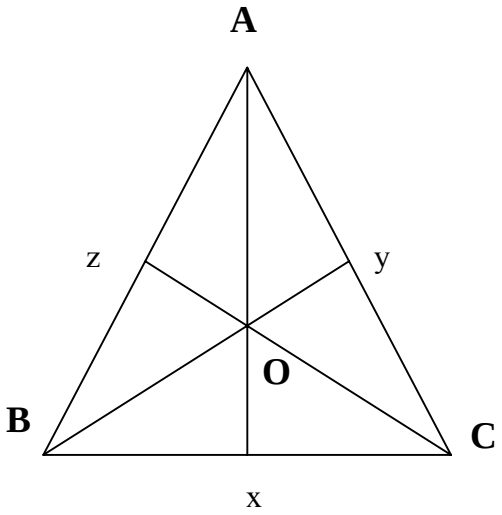

Figure 4: Symmetries of an Equilateral Triangle.

- X means 'Reflect in the line x.'
- Y means 'Reflect in the line y.'
- Z means 'Reflect in the line z.'
- R means 'Rotate by 120^o anticlockwise about O.'
- S means 'Rotate by 240^o anticlockwise about O.'
- I means 'Do nothing.'

	I	***R***	***S***	***X***	***Y***	***Z***
I	*I*	*R*	*S*	*X*	*Y*	*Z*
R	*R*	*S*	*I*	*Z*	*X*	*Y*
S	*S*	*I*	*R*	*Y*	*Z*	*X*
X	*X*	*Y*	*Z*	*I*	*R*	*S*
Y	*Y*	*Z*	*X*	*S*	*I*	*R*
Z	*Z*	*X*	*Y*	*R*	*S*	*I*

Table 4: Dihedral Group D_3 Formed by the Symmetries of an Equilateral Triangle