LAGRANGE'S THEOREM

Sharon Donohoe and Ciara Hamilton†
†National University of Galway

INTRODUCTION

This poster will discuss one of the Lagrange's lasting legacies;
Lagrange's theorem on groups, as well as the developments it underwent to become the theorem we recognise today.

Lagrange's theorem is a well known result which is used in group theory and other fields in mathematics, it is defined as followed:
"Let G be a group of order n and H a subgroup of order m. Then m is a divisor for n"

WHO WAS LAGRANGE?

Joseph-Louis Lagrange was an Italian mathematician born in Turin in 1736.
By age 19, Lagrange had become a professor of mathematics Royal Artillery School in Turin.
Due to his prolific contributions to mathematics and physics, he soon became known as one of the greatest mathematicians in Europe.
Lagrange was born into a changing world in 18th century Italy.
Growing up he was surrounded by great developments in medicine, physics, and the natural sciences, pioneered by his fellow Italian scholars.
There is no doubt that Lagrange soon went on to become one of the defining academics of the age of enlightenment in Italy.

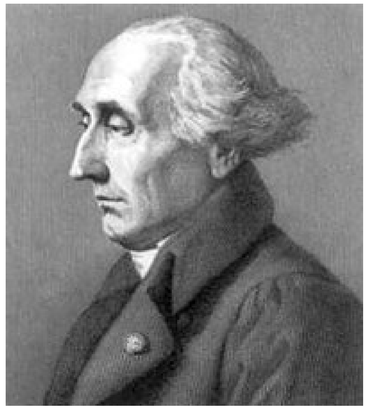


Fig. 1: Joseph-Louis Lagrange.

SOME IMPORTANT DEFINITIONS

GROUP: a non-empty set equipped with a binary operation that together satisfy the properties of closure, associativity, the identity property, and the inverse property.

SUBGROUP: Suppose G is a group under the operation *, and let H be a subset of G. Then H is a subgroup of G if H satisfies the four properties of a group under the operation of G.

ORDER: the order of a group is the number of elements in its set.

ORIGINAL THEOREM OF LAGRANGE

When Lagrange first proposed his theorem, group theory had not yet been defined.
The theorem was first developed in 1770 when Lagrange published workings on the theory of equations.
In this he aimed to derive a formula that could be used to solve a polynomial of 5 degrees or higher.
He reasoned that if solving the quadratic and cubic polynomials involved solving supplementary polynomials of a lower degree then the same might stand for a polynomial of the 5th degree.
This led to the original theorem which stated: If a function F(x1, x2, . . . , xn) of n variables is acted on by all n! possible permutations of the variables and these permuted functions take on only r distinct values then r is a division of n.
This original theorem is vastly different from the one we know today. As the study of group theory developed and changed so too did the theorem originally propose by Lagrange back in 1770.

DEVELOPMENTS ON HIS WORK

Many later developments were made on Lagrange's original work.
In 1799, Paolo Ruffini published a book in which he provided proof that the converse of Lagrange's Theorem does not hold.
In 1815, a paper by Cauchy tied together the prior developments made on Lagrange's Theorem. Cauchy provided a proof of the original theorem as well as a generalised version of Ruffini's theorem.
Cauchy later went on to prove that order of a subgroup Sn is a divisor of n!.
This was the first solid proof of Lagrange's theorem in the case of symmetric groups.
It wasn't until the twentieth century that the language of cosets was used to prove Lagrange's theorem.
Though it is hard to accredit anyone in particular with the first formal proof of the theorem, the coset approach is said to have been inspired by Galois.

Fig. 2: Austin Louis Cauchy

PROVING LAGRANGE'S THEOREM

In order to proof Lagrange's theorem we start with a subgroup H of the finite group G.
If we find that H = G then the theorem holds.But if H G then we choose an element x of G with x not being an element of H (xH).
Then the coset xH is disjoint from H and has |H| elements. If H xH = G then |G| = 2|H| and we are done.
If not, choose y 6 H xH and add the coset yH.Eventually we find that G is the union of k disjoint left cosets of H, and |G| = k|H|.

THE THEOREM EXPLAINED

In this case the term "divides" tells us that the order of subgroup H is a factor of the order of group G.
An example of the theorem in practice is the group S4. S4 has 4! (or 24) elements.
A subgroup of S4 could possibly have 1,2,3,4,6,8,12, or 24 elements as these are all factors of 24 (the order of S4).
The subgroup could not have, for example, 9 or 11 elements as these do not divide 24.
The converse of the theorem is not true.

APPLICATIONS OF LAGRANGE

Lagrange Theorem can be widely applied in mathematics's to prove other theorems.
This can be used to prove Euler's theorem and Fermat Theorem (an integer raised to a prime power leaves the same remainder as the integer itself when divided by the prime) and its generalization.
In addition to this we can use Lagrange to illustrate that there are infinitely many primes.
Lagrange's Theorems can be seen today used in the modern world of the digital payments system namely Cyptocurrencies (eg.Bitcoin).

THE FUTURE OF LAGRANGE

The Future of Lagrange lies in the hands of two very capable students of the School of Mathematics at NUI Galway.

References

Moravia, Sergio., 'An Outline of the Italian Enlightenment', in Comparative Literature Studies, vol. 6, no. 4 (1969), pp.380-409.

Roth, Richard L., 'The History of Lagrange's Theorem on Groups', in Mathematics Magazine, vol. 74, no. 2 (April 2001), pp. 99-108.

'Joseph-Louis Lagrange',Physics Today, (January 2017), https://physicstoday.scitation.org/do/10.1063/PT.5.031404/full/, accessed

Card Shuffling as a Group and the Faro Shuffle

Anna Golden, Emma Meaney, Lise Wall, Lydia Costello

Introduction

In this poster we look at card shuffling a deck of cards is as a group. First, we establish that shuffling is a group and that it is isomorphic to the group of permutations S_N where N is the number of cards in a deck, typically 52 in a standard deck. We then discuss a specific type of shuffle known as the Faro or Perfect Shuffle used by magicians and gamblers, that has interesting properties when considered as a group. We prove the Fundamental Theorem of Faro Shuffling. We discuss the generating set of shuffles. We give an example of a card trick that applies these concepts.

Why Is Card Shuffling a Group?

The set of all shuffles can be represented by the symmetric group S_N, where N is the number of cards in the deck.Let S be a card shuffle that acts on S_{52}, such that S:1,2,...,52 ↦ 1,2,...,52 (Let T, U also be shuffles on S_{52}). The shuffling function is a form of permutation. Card shuffling is a group because it satisfies the group axioms as follows:

- **Closure:** consider shuffles (permutations) S,T, then S ∘ T is also a shuffle (perform T, followed by S)
- **Identity:** This consists of the shuffle which leaves each element in it's original position. Let i(x) be the identity shuffle performed on x ∈ 1,2,...,52, then i(1)=1, i(2)=2,...,i(52)=52.
- **Inverse:** Each permutation S also has an inverse S^{-1} contained in the group, e.g if S(1)=52, $S^{-1}(52)$=1.
- **Associative Property:** For shuffles S,T,U it is true that:
  - S ∘ (T ∘ U) = (S ∘ T) ∘ U.

Faro/Perfect Shuffle

The Faro shuffle is a method of "perfectly" shuffling a deck of cards. A deck of cards is divided into two equal piles and then perfectly interwoven. There are two ways of doing this:

- **In Shuffle:** The In Shuffle leaves the top and bottom card second from top and bottom respectively.

$$\begin{pmatrix} 1 & 2 & 3 \dots 25 & 26 & 27 \dots 50 & 51 & 52 \\ 2 & 4 & 6 \dots 50 & 52 & 1 \dots 47 & 49 & 51 \end{pmatrix} \tag{1}$$

- **Out Shuffle:** The Out Shuffle leaves the top and bottom card in place.

$$\begin{pmatrix} 1 & 2 & 3 \dots 25 & 26 & 27 \dots 50 & 51 & 52 \\ 1 & 3 & 5 \dots 49 & 51 & 2 \dots 48 & 50 & 52 \end{pmatrix} \tag{2}$$

By doing a Faro shuffle on a memorized deck, one can always compute where a card in any given position will end up. What is perhaps more interesting is that Faro shuffles form a subgroup and will always return to the identity within a set number of shuffles. As we will see, for a deck of 52 cards, it will take exactly eight Faro Shuffles to return the cards to their original positions (i.e. $\text{Faro}^8 = id_{52}$).

The Fundamental Theorem of Faro Shuffling

Alex Elmsley found that a series of in and out shuffles can be used to bring the original top card (at position 0) to any desired position p in the deck. This can be achieved by expressing p in binary with 0 meaning an out shuffle and 1 meaning an in shuffle. For example to go from 0 to position 7 (where 7 = 111), perform in, in, in.

With a deck of $2n$ cards, r exists such that $2^{r-1} < 2n \leq 2^r$.
Where $0 < p < 2n-1$, let $t = \frac{(p+1)2^r}{2n}$.
For $p = 0$, set $t = 0$. For $p = 2n-1$, set $t = 2^r - 1$.
Express t in binary as $t = t_{r-1}t_{r-2}...t_1t_0$ with $t_i = 1$ or 0
Let s be correction terms where $s = 2nt - 2^r p = s_{r-1}s_{r-2}...s_1s_0$ with $s_i = 1$ or 0
The shuffling sequence is $t_{r-1} + s_{r-1}, t_{r-2} + s_{r-2}, ..., t_0 + s_0$

For example, if $2n = 52, p = 35$. Then $r = 6$, $t = \frac{36(64)}{52} = 44 = 101100$ and $s = 2288 - 2240 = 48 = 110000$.
Now the co-ordinate sum of 101100 and 110000 is 011100 which is out, in, in. We can ignore the final two shuffles as they do nothing to the top card.

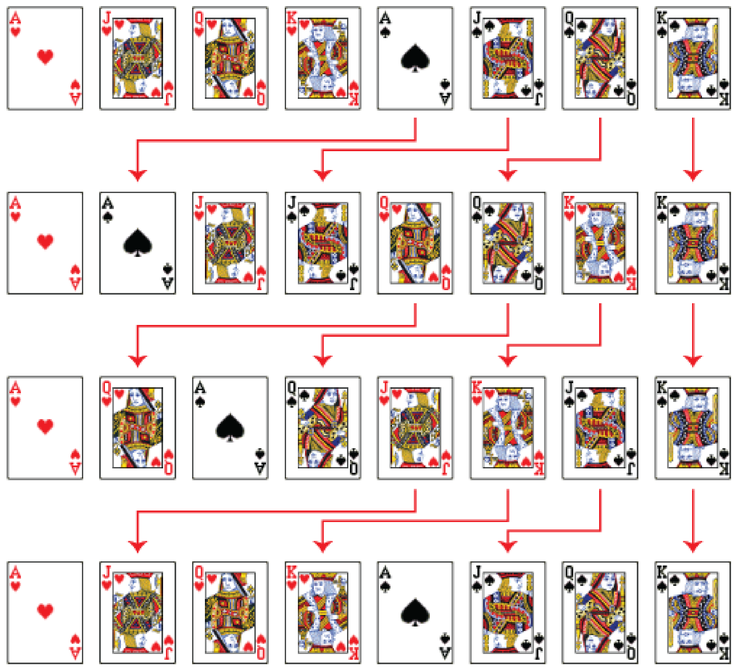


Fig. 1: For an 8-card deck, only three out-shuffles are required to restore the original order

The Generating Set of Shuffles

Starting with a randomly shuffled deck of 52 cards, any other shuffle of the deck can be reached by a combination of swapping the first two cards and putting the bottom card on top of the deck. In other words S_{52} is generated by the transposition (1 2) which swaps the first two cards in the deck and the 52-cycle (1 2 ... 52) which brings the bottom card of the deck to the top.
Proof:

Let x = (1 2 ... 52)

$$\begin{aligned}
&x(1 \quad 2)x^{-1} = (2 \quad 3) \\
&x(2 \quad 3)x^{-1} = (3 \quad 4) \\
&\vdots \\
&x(50 \quad 51)x^{-1} = (51 \quad 52) \\
&\implies (i \quad i+1) \in \langle (1 \quad 2), x \rangle \quad \forall \quad 1 \leq i \leq 51 \\
&(2 \quad 3)(1 \quad 2)(2 \quad 3)^{-1} = (1 \quad 3) \\
&(3 \quad 4)(1 \quad 3)(3 \quad 4)^{-1} = (1 \quad 4) \\
&\vdots \\
&(51 \quad 52)(1 \quad 51)(51 \quad 52)^{-1} = (1 \quad 52), \\
&\implies (1 \quad i) \in \langle (1 \quad 2), x \rangle \quad \forall \quad 1 \leq i \leq 52 \\
&\text{For any} \quad 1 \leq i < j \leq 52 : \\
&(i \quad j) = (1 \quad i)(1 \quad j)(1 \quad i)^{-1} \in \langle (1 \quad 2), x \rangle.
\end{aligned}$$

Therefore $\langle (1,2), x \rangle$ generates all transpositions in the group S_{52}, and so generates the group itself as every permutation is a product of transpositions.

A Card Trick to Try

Before you start memorise the card on the bottom of the deck. Ask your friend to pick a card out of the deck, look at it and put it on top of the deck without you seeing it. Then allow them to cut the deck as many times as they want. Spread the cards out face up and announce the chosen card which is the card in front the "bottom card" you had memorised.
Why does this work?
Under the action of cutting the cards the adjacency of pairs of cards is preserved. The group H is the subgroup of S_{52} generated by the 52 cycle (1 2 3... 51 52). The adjacency of pairs of cards is not changed by any action in H and so although H seems to be shuffling the cards, the chosen card will always remain in front of the original bottom card making it is easy to find the chosen card.

References

Conrad, K.,Generating Sets. University of Conneticut.https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf
C-for-dummies.com.2017.The Perfect Shuffle | C For Dummies Blog.[online]https://c-for-dummies.com/blog/?p=2519
Diaconis, P., Graham, R. and Kantor, W.(1983). The mathematics of perfect shuffles. Advances in Applied Mathematics, 4(2), pp.175-196.
Diaconis, P. and Graham, R.(2020). The Solutions To Elmsley'S Problem.https://statweb.stanford.edu/~cgates/PERSI/papers/pre-elmsley.pdf
Ensley, D. (1999). Invariants under Group Actions to Amaze Your Friends. Mathematics Magazine, [online] 72(5), p.383.https://www.maa.org/sites/default/files/269079545577.pdf
Quinlan, R. (2020), "The Axioms of a Group", *MA3343: Groups*, available: http://www.maths.nuigalway.ie/~rquinlan/groups/section1-2.pdf [accessed 11 Dec 2020]

Group Theory applied to the Rubik's Cube

Thomas Jackson Aibhilín Crangle Ronan Finnegan

Introduction

In our 3rd year project of Group Theory, we decided to see how all the information we learned in this module applies to the Rubik's Cube, a puzzle designed by the teacher and puzzler Erno Rubik in 1974.

Proof the Permutations of a Rubik's Cube are a Group

The 4 axioms that must be fulfilled in order to be a group are closure, associativity, identity and inverse.

- Closed Property : If A and B are operations then A*B is an operations as well.
- Associativity : For all A, B, C in G, one has (A*B)*C = A*(B*C))
- Identity Property : The identity id. can be defined as the move that does not perform any rotations and remains as is.
- Inverse Property : For each A in G, there exists an element B in G such that A*B = id., and B*A = id., where id. is the identity element.

Notation of the Rubik's cube

Generally, the actions on a Rubik's cube are notated as follows:

F - rotate the front side of the cube 90° clockwise
B - rotate the back side of the cube 90° clockwise
L - rotate the left side of the cube 90° clockwise
R - rotate the right side of the cube 90° clockwise
U - rotate the top side of the cube 90° clockwise
D - rotate the bottom side of the cube 90° clockwise

Placing a ' after the letter implies you rotate the face *anticlockwise* instead e.g. F' would mean rotate the front face anticlockwise.

Placing a '2' after the letter implies rotation by 180° instead. e.g. B2 means rotate the back face 180°.

Subgroups of the Rubik's Cube

A *subgroup* of a group is simply a subset of the group that also satisfies the group axioms. (closed, inverse, etc.)

For example, define S to be:

$$S := \{id, L, L2, L'\}$$

Then S is a subgroup of the whole group.

- S is clearly a subset of the group
- S contains the group identity
- The composition of 2 elements in S is also in S (e.g. L*L2 = L')
- Every element in S can be undone by another element of S (or in the case of L2, itself)

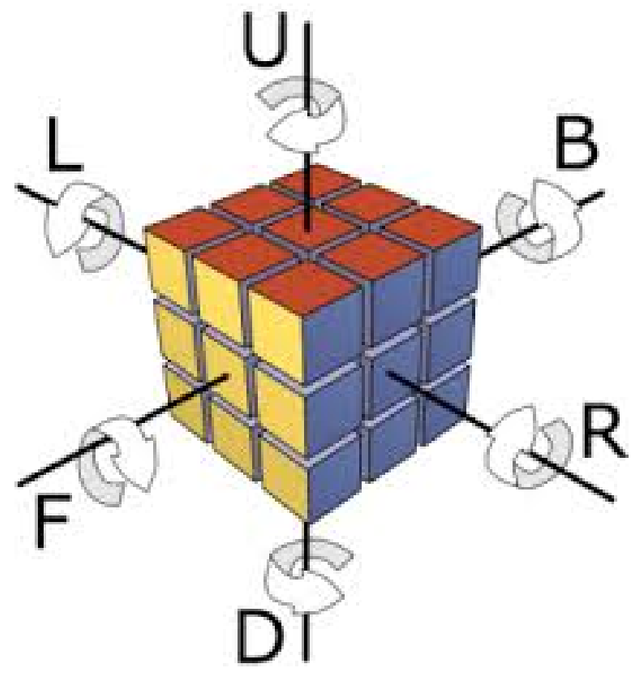
Commutativity and Centre of the Rubik's Cube

A group is *commutative* if a*b = b*a for all a, b $\in$ *G*. Such groups are known as *abelian*.

The Rubik's Cube Group is not abelian. If we rotate our L axis and then our F axis both in a clockwise direction, we cannot return to our original position just by repeating those moves in reverse order.

The *centre* of a group is the set of elements that commute with EVERY element in the group. In our Rubik's Cube, the centre of the group consists only of our identity element and a move known as the "Super Flip"

The Notations of the Rubik's Cube



The Super Flip

The Super Flip of any Rubik's Cube is a series of 20 moves that, when completed, transforms the cube so that the corners and centre of each face remain in the same position, but the edge pieces ("cubies") are flipped. If we were to complete the Super Flip twice, we get our original cube (The Super Flip has order 2).

Super Flip: U*R2*F*B*R*B2*R*U2* L*B2*R*U'*D'*R2*F*R'*L*B2*U2*F2

Orbits of the Rubik's Cube

The *orbit* of a point (e.g. face, corner, or even one of the cubies) of the cube under a group is every position that point can be in under the action of the group.

For example, each of the corner cube form an orbit under the whole group, as each corner cube can only be moved to another corner. The order of this orbit is 8 as there are 8 corners.

Similarly, the "cubies" form an orbit of order 12.

Finally, the centre squares don't change position (apart from rotating, but this is irrelevant), so its orbit size is just 1.

Stabilizers of the Rubik's Cube

The *stabilizer* of a point under a group is every element of the group that keeps that point exactly where it is.

For example, performing any of B, B2, or B' wont move any of the faces on the front side of the cube, so we say B, B2 and B' are in the stabilizer of these faces.

References

https://ruwix.com/
https://en.wikipedia.org/wiki/Rubik's_cube
https://www.youtube.com/watch?v=BTyzE-NDga8
http://people.math.harvard.edu/ jjchen/docs/rubik.pdf

Quantum Mechanics: The Stabilizer Formalism

Billy Ray

Introduction

The stabilizer formalism of quantum mechanics presents a novel way of describing the machinery of quantum mechanics using concepts from Group Theory. The stabilizer formalism uses the concepts of the stabilizer of a group and generators of a group in order to characterise quantum states and the result of operations on those states.

Quantum States

- Quantum states are represented as unit vectors in a complex vector space. The state is represented using a set of orthonormal basis vectors which span the space. Let $|0\rangle$ and $|1\rangle$ represent a basis of two orthonormal vectors in $\mathbb{C}^2$ such that:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  Thus, a quantum state, $|\psi\rangle \in \mathbb{C}^2$, could have the form:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

- A quantum state in $\mathbb{C}^2$ is called a qubit state. The basis of quantum computing consists in manipulating qubit states through matrix-vector multiplication.

Multiple Qubit States

- The tensor product operation combines multiple qubits into a single composite system. The composite system of two qubits, $|\psi\rangle \otimes |\psi\rangle$, occupies the complex vector space $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$. Thus, a 2-qubit state can be represented using a set of four orthonormal basis vectors spanning the space $\mathbb{C}^4$.
- In general, a composite system of n qubits is defined in $\mathbb{C}_1^2 \otimes \mathbb{C}_2^2 \otimes ... \otimes \mathbb{C}_n^2 = \mathbb{C}^{2^n}$. An arbitrary n-qubit state can be represented using an orthonormal basis consisting of 2^n vectors which span the vector space $\mathbb{C}^{2^n}$.

The Pauli Group

- Operators are matrices which act on quantum states. Operators acting on separate qubit states are also combined using the tensor product operation. For two operators U_1 acting on a qubit $|\psi_1\rangle$ and U_2 acting on another qubit $|\psi_2\rangle$, the total action on the composite system is simply:

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1 |\psi_1\rangle \otimes U_2 |\psi_2\rangle)$$

- For the qubit state, $|\psi\rangle \in \mathbb{C}^2$, there exist a special class of operators known as the Pauli matrices:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- A group under the operation of matrix multiplication, known as the Pauli group, G_1, can be defined using these operators with the multiplicative factors ± 1 and $\pm i$:

$$G_1 = \{\pm\mathbb{I}, \pm i\mathbb{I}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

  The Pauli group generalizes to the n-qubit case, where each element of the Pauli group, G_n, is a distinct tensor product of n individual Pauli matrices with multiplicative factors ± 1 and $\pm i$[1].
- Every matrix in the group G_1 can be *generated* by the elements X,Y and Z:

$$G_1 = < X, Y, Z >$$

The Stabilizer Formalism

- Consider a subgroup S of G_n, and define the subspace V_s to be the set of n-qubit states which are fixed by every element of S. The set of vectors V_s is *stabilized* by S and the subgroup S forms the *stabilizer* of the subspace V_s, $Stab_{G_n}(V_s)$.
- The subgroup S can be defined in terms of its *generators*. To assess whether a particular n-qubit state belongs to the stabilized subspace, V_s, it suffices to check whether the vector is stabilized by the generators of S[1].

Arbitrary Operations

- Quantum operators are unitary, this means they satisfy the relation $UU^\dagger = U^\dagger U = \mathbb{I}$ where U is a unitary operator and $U^\dagger$ involves transposing U and complex conjugating all of the entries.
- Consider an arbitrary unitary operator, U, applied to the vector space V_s which is stabilized by the subgroup S. For any vector $|\psi\rangle \in V_s$ and matrix element $g \in S$ we find:

$$U|\psi\rangle = Ug|\psi\rangle = (UgU^\dagger)U|\psi\rangle$$

- The new vector $U|\psi\rangle$ is stabilized by $UgU^\dagger$. After applying the operator U to our entire vector space V_s, we can see that our new vector space UV_s has stabilizer $USU^\dagger = \{UgU^\dagger | g \in S\}$.
- If the stabilizer S has generators $< g_1, g_2, ..., g_n >$ then our new stabilizer, $USU^\dagger$, has generators $< Ug_1U^\dagger, Ug_2U^\dagger, ..., Ug_nU^\dagger >$.

Benefits of the Stabilizer Approach

- It can be shown that the Pauli Z gate stabilizes the $|0\rangle$ state i.e. $Z|0\rangle = |0\rangle$. Thus, an n-qubit state:

$$|\phi\rangle = (|0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |0\rangle_n) = |0\rangle^{\otimes n} \in \mathbb{C}^n$$

  has a stabilizer with a single element, $S = \{Z_1 \otimes Z_2 \otimes ... \otimes Z_n\}$.
- Define a unitary operator, H, with the property $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Applying this operator to $|\phi\rangle$ gives:

$$H^{\otimes n}|\phi\rangle = H_1|0\rangle_1 \otimes ... \otimes H_n|0\rangle_n \in \mathbb{C}^{2^n}.$$

- However, the Pauli X gate stabilizes this resulting state:

$$X\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- This means our new state $H^{\otimes n}|\phi\rangle$ also has a single-element stabilizer, $S' = \{X_1 \otimes X_2 \otimes ... \otimes X_n\}$. Our stabilizer still has n terms, but the vector representation of our new state has 2^n terms! For 100 qubits, this is a $\approx 10^{28}$ improvement...
- A group-theoretic approach to simple quantum computations allows for classical simulations as we can keep the number of terms *linear* in n.

References

Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

History of Lagranges Theorem

By Dylan Cassidy Killane and Cian Forde

National University of Ireland, Galway

Introduction

Joseph Louis Lagrange and his theorem are core principals to grouping theory. Through this informative poster we intend to examine the history of this theorem including:

- A brief history on the creator Joseph Louis Lagrange
- Why did he create this theorem?
- Other famous mathematicians' contributions to the theorem
- Examples of this theorem
- Applications of the theorem in today's world

Joseph Louis Lagrange - The Man Behind The Theorem

Joseph Louis Lagrange was born on the 25th of january 1736 in Turin. He studied at the University of Turin where his favourite subject was classical Latin having no great enthusiasm in mathematics and found Greek Geometry rather dull and in his later life is famously quoted as saying "If I had been rich, I probably would not have devoted myself to mathematics".[1] After having his interest in mathematics sparked by reading a paper published by Edmond Halley. From this he improved his stature in the world of mathematics with feats like solving the isoperimetrical problem at only 19 years of age. Then in 1766 he moved to Berlin to start work on his theorem of which is named after him, Lagrange's Theorem. Later in life he moved to France and became a naturalised frenchman. He would pass away in Paris in April 1813.

NUI Galway
OÉ Gaillimh

What was he trying to achieve?

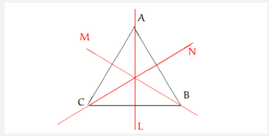
With formulas already existing for the quadratic, cube and quartic equations, Lagrange wanted to derive a formula for equations of degree five also known as quintic equations and more specifically for equations of nth degree. He saw that when solving more known polynomials such as quadratic and cubic resolvent polynomials of lesser degrees. From this he noted that the roots of the polynomial x1,x2,x3 and x4 could be permuted 24 times or (4!)

Other Famous Mathematician's Contributions

Augustin-Louis Cauchy contributed twice to Lagrange's theorem writing a paper on permutation groups before the idea of groups was even formalised and again in 1844, proving lagranges theorem for symmetric groups.
Camille Jordan added to Cauchy's work in 1861 by proving the theorem for finite permutation groups
Evariste Galois was the man who formalised the idea of groups in 1831 in a paper on solving solutions of permutation groups by radical

Examples of this Theorem

- Lagrange's Theorem: If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.
- Let D6 be the set of symmetries of the equilateral triangle, with rotations id, R120, R240 and reflections TL, TM and TN as shown.[2]



- Then H = id, TL is a subgroup of D6 of order 2, and left cosets of H in D6 determined by the six elements are:
  1. idH = id ∘ id, id ∘ TL = id, TL = H
  2. TLH = TL ∘ id, TL ∘ TL = TL, id = H again.
  3. R120H = R120 ∘ id, R120 ∘ TL = R120, TM.
  4. TMH = TM ∘ id, TM ∘ TL = TM, R120 = R120H again.
  5. R240H = R240 ∘ id, R240 ∘ TL = R240, TN
  6. TNH = TN ∘ id, TN ∘ TL = TN, R240 = R240H again.

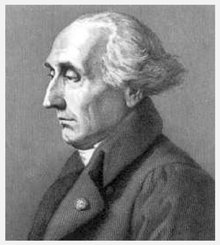


Figure: Joseph Louis Lagrange

Contributors To This Theorem

Figure: Cauchy(left), Galois(Centre), Jordan(right)

Application in Todays World

- It seems fair to state that Lagranges theorem is going to be used a lot more in the everyday life of a mathematician than that of say an electrician. If you are a mathematician however its applications are bountiful. For example, Lagranges theorem can be used to prove Euler's theorem as well as Fermat's little theorem aswell as its generalization.[3]
- It also has uses in cryptography.Due to its use in computing the power of an integer modulo a prime number. This shows the theorem to be applicable even in the general public's lives whether they know it or not as cyber-security plays such an important part in our lives.

Conclusion

Lagrange is such an interesting Mathematician to study to say the least. It seems bizzare that someone so intelligent and mathematically skilled had no great passion for his field of study. Inspite of this he has produced one of the most important theorem's used in Group theory to this day. It's core use in group theory will preserve Lagranges name in the minds of mathematicians for centuries to come.

References

[1] J. J. O'Connor and E. F. Robertson. Joseph louis lagrange. https://mathshistory.st-andrews.ac.uk/Biographies/Lagrange/, January 1999.

[2] Essential concepts of group theory. http://www.maths.nuigalway.ie/~rquinlan/groups/section2-1.pdf.

[3] Lagranges theorem (group theory) wikipedia. https://en.wikipedia.org/wiki/Lagrange%27s_theorem_(group_theory).

Frieze Groups

Thomas Hayes Cian Doheny Jack Flood

Introduction

Our chosen topic is frieze groups. Frieze groups are two-dimensional line groups, having repetition in only one direction. They are the distancing preserving transformations of a pattern.

What makes a frieze group

There are seven distinct frieze groups. All of them can be generated by translation, reflection (along the same axis) and a 180° rotation.
The seven Frieze groups are:

- The first frieze group F_1 was named by Conway as a HOP. 
- The second frieze group, F_2, contains translation and glide reflection symmetries. According to Conway, F_2 is called a STEP. 
- The third frieze group, F_3, contains translation and vertical reflection symmetries. Conway named F_3 a SIDLE. 
- The fourth frieze group, F_4, contains translation and rotation (by a half-turn) symmetries. According to Conway, F_4 is called a SPINNING HOP. 
- The fifth frieze group, F_5, contains translation, glide reflection and rotation (by a half-turn) symmetries. Conway calls F_5 a SPINNING SIDLE. 
- The sixth frieze group, F_6, contains translation and horizontal reflection symmetries. Conway named F_6 a JUMP. 
- Finally, the seventh frieze group, F_7, contains all symmetries (translation, horizontal vertical reflection, and rotation). According to Conway, F_7 is named a SPINNING JUMP. 

[1]

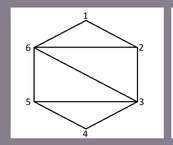
Background and History of frieze groups

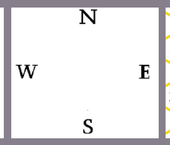
Frieze patterns name originated from the architectural term of a frieze or a broad decorative band and were extremely popular in Ancient Greece. The patterns started off as simply patterns of lines repeated all the way around the building, with each set of lines spaced a particular distance away from the previous one. Later on the patterns became more intricate involving moldings or painting in each of the spaces where the lines used to be, but it would still be the same image repeated all the way around the structure. [2]

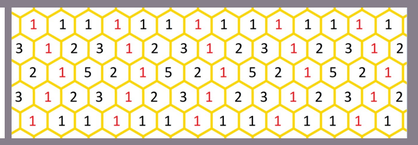
Frieze Pattern

Imagine some $n-gon$. Another way of looking at Frieze pattern is as a table of Natural numbers displayed in a lattice. Where the top and bottom rows are 1's, and the amount of rows is determined by $n-3$. To figure out the second row we triangulate the $n-gon$(hexagon in this example) any way we wish. Making some order out of the vertices(clockwise in this example), the number in the pattern corresponds to the amount of triangles adjacent to that vertex . The following rows are calculated by making unit diamonds with the above two rows labeling vertices in a compass fashion N,S,E,W.

$$(W \times E) - (N \times S) = 1$$



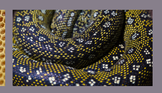




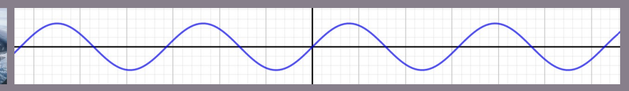
The example portrayed here is a special *Lightning bolt* example named due to the 'lightning bolt' of 1's

Examples of frieze groups in the real word

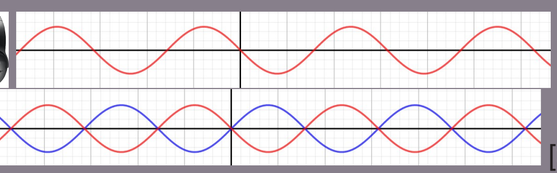
There are natural and man made friezes all around us. The honeycomb in a bees' nest (left) is an example of F_1 layered on top of each other. Snake skins have amazing intricate frieze patterns. This snake skin pattern (right) contains all symmetries. What Frieze groups can you spot in the honeycomb?



If we can think of a constant sound, like the engine on a plane, wave we can see examples of different frieze groups. If we take our first space as one period of a wave we can then see an example of F_1. If we take our second space as a quarter period of a wave we can then see an example of F_5.



An example of where we see similarities to Frieze groups are destructive sound waves, these are waves generated by headphones to cancel out background noise. Destructive waves looks like F_6 applied to the sound wave resulting in the inverted shape to cancel out noise(red graph). The resulting waves when added together(played together) should look like the final graph(red and blue) called total destructive interference.



[3]

References

URL: https://www.maa.org/sites/default/files/images/upload_library/4/vol1/architecture/Math/seven.html.

Tyler Landau. *Classifications of Frieze Groups and an Introduction to Crystallographic Groups*. 2019. URL: https://www.whitman.edu/documents/Academics/Mathematics/2019/Landau-Balof.pdf.

Numberphile. URL: https://www.youtube.com/watch?v=0mXz-NP-raY.

THE CONVERSE OF LAGRANGE'S THEOREM

Megan McGlinchey and Eoin Mulvihill

Group Theory MA3343

Introduction

Lagrange's Theorem can be regarded as one of the most central theorems of abstract algebra and considered by many "the most important theorem of group theory". However, the converse of this infamous theorem is undoubtedly false. This poster will explore why the converse fails as well as other methods of finding subgroups

Joseph Lagrange

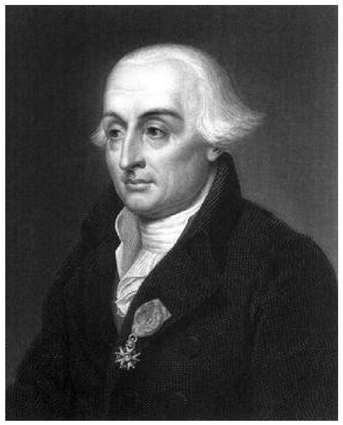


Fig. 1: Joseph Lagrange.

Giuseppe Luigi Lagrange was born in Turin, Italy on 25th January 1736. He made many significant contributions towards analysis, number theory and analytical and celestial mechanics although, sadly, did not prove his own theorem. In 1801 Gauss proved Lagrange's theorem for the multiplicative group of non-zero integers modulo p, $(\mathbb{Z}_{/p}\mathbb{Z})$, in 1844 Cauchy proved the theorem for the symmetric group S_n and, finally, Jordan proved Lagrange's theorem for the case of any permutation group in 1861.

Applications of his work

Lagrange's Theorem displays some key properties that allow for further theorems such as Fermat's little theorem and Wilson's theorem to be proven as well as showing there to be infinitely many primes.

Converse of Lagrange's Theorem

Every divisor of the order of group G is the order of some subgroup H of G

Where the converse fails

The most basic example to demonstrate where the converse fails, is the alternating group A_4 of even permutations.

A_4={ ID,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(123),(132),(124),(142),(134),(143),(234),(243)}

$|A_4|$=12 , With the divisors of the group being {1,2,3,4,6,12}

Lets assume there exists a subgroup H, in A_4 with the order of $|H|$=6.
Let V be a non-cyclic subgroup of A_4 –> Known as the Klein four group.
V={ID,(12)(34),(13)(24),(14)(23)}

Let $K = H \cap V$, Since H and V are subgroups of A_4, then so to is K.
By Lagrange's Theorem, K's order divides both 6 and 4. So $|K|$=1 or $|K|$=2

If $|K|$=1, the map $\big(h, v\big)$ -> $h.v$ defined from H x V to A_4 has a one to one relationship implying A_4 has 24 elements which we know is not true.
So $|K|$ = 2 where $h \in H$ and $v \in V$

The index $|A_4 : H|$=2 shows that there is exactly 2 distinct cosets and as such, we know H is a normal subgroup.
This implies $H = tHt^{-1}\ \forall t \in A_4$.

Take $v = \big(ab\big)\big(cd\big)$ and $t = \big(abc\big)$, where $\big(a, b, c, d\big)$= (1,2,3,4)
tvt^{-1} = $\big(bc\big)\big(ad\big) \neq \big(ab\big)\big(cd\big)$
$tvt^{-1} \neq v$
but V contains all disjoint transpositions so,
$tvt^{-1} \in V$ and $tvt^{-1} \in H$ So, $tvt^{-1} \in H \cap V = K$. Thus, we have demonstrated that there is a third element in K which contradicts our assumption that $|K|$=2 and so there is no subgroup of order 6.

Cauchy's Theorem

Cauchy's Theorem states that a group G whose order g is divisible by a prime number p contains an operator of order p.
Proof:
Suppose G is abelian and generated by a single operator S of order np. $S^n \neq 1$ although $(S^n)^p = 1$, showing that S^n is the required operator. If G is not generated by a single operator, we can examine a set of generating operators $\{S_1, S_2, ..., S_r\}$, which are all commutative. Since these operators are commutative there exists at least one generator for which the order is divisible by p, and some power of this generator must be the required operator of order p.

Fig. 2: Augustin-Louis Cauchy.

References

- Miller, G.A.. (1898). On an Extension of Sylow's Theorem. Bull. Amer. Math. Soc., vol. 4 p323
- https://mathshistory.st-andrews.ac.uk/Biographies/Lagrange/
- https://www.maa.org/sites/default/files/pdf/cms$_upload/On_the_Converse-Gallian34078.pdf$

- https://www.mathcounterexamples.net/converse-of-lagrange-theorem-does-not-hold/

- https://en.wikipedia.org/wiki/Lagrange

Group Theory

Applications of Non-Abelian Groups in Cryptography

Emma Corbett, Eoin McArdle & Gordon O'Connor

National University of Ireland, Galway

Introduction

Currently the majority of cryptographic schemes are based on commutative algebraic structures such as Abelian Groups. In terms of classical computing, these schemes are considered secure. This is because the problems which underpin their operation are considered 'hard' or intractable. This means that no solution can be found in reasonable time. For example it takes approx. $2.73 * 10^{61}$ years to crack AES-256 encryption using a home computer. However, recent advancements in quantum computing theory have shown that not all these problems are indeed intractable. The use of non-commutative algebraic structures such as non-abelian groups offer a possible solution to this security issue.

Abelian Groups in Cryptography

Abelian Platform Groups:

Many abelian groups can be used for cryptographic schemes. A simple example is the additive group $G = \mathbb{Z}/d\mathbb{Z}$. However, in practice much larger and complex groups are used. Groups of points on suitable elliptic curves are usually used. An elliptic curve is given by the equation $y^2 = x^3 + ax + b$.

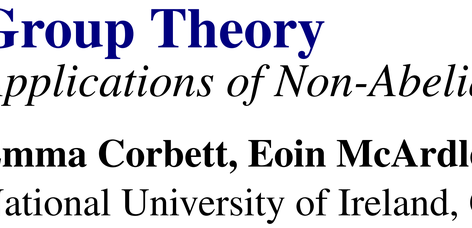


Figure 1: Examples of an Elliptic Curves

Discrete Logarithm Problem (DLP):

The DLP is one of the main problems that current crypography relies on. It is described as follows where G is a cyclic group with generator g:

$$\textit{Let } G = \langle g \rangle$$

$$\textit{Given } h \in G \textit{ find } x \textit{ such that } g^x = h$$

- Currently the DLP problem is intractable using current computing methods for certain large groups of G.
- However, Shor's quantum algorithm has been shown to solve this problem in polynomial time, therefore making the DLP tractable even for complex, large groups such as elliptic curves.
- *Fig. 2* shows the difference between tractable problems (polynomial, linear, logarithmic) and intractable problems (exponential) in terms of time.

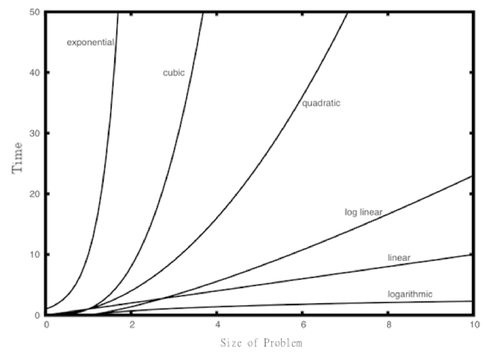


Figure 2: Time Complexity

Diffie-Hellman Key Exchange:

The Diffie-Hellman Key Exchange protocol is a fundamental method of establishing a secret shared key between two parties over an insecure connection. Suppose Alice and Bob wish to create a shared key, K using the cyclic group G where the order, d, and generator, g of G are publicly known:

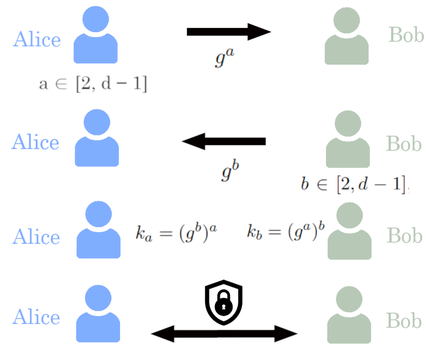


Figure 3: Diffie-Hellman Protocol

- From the above protocol we can clearly see that the Diffie Hellman Key Exchange relies on the DLP being intractable as do many other cryptographic protocols.
- This highlights the need for a more secure alternative for the quantum computing age.

Non-Abelian Platform Groups

The idea of using the complexity of non abelian (infinite) groups in cryptography dates back to the work of Wagner and Magyairk in 1985. A cryptographic platform group G must have several key requirements in order to tackle the conjugacy search problem:

- The group G must be well studied/understood.
- The word problem in G should have a linear/quadratic solution by a deterministic algorithm.
- There should be a way to disguise the elements of G so that they it is impossible to to recover individual elements from a product of elements just by inspection.
- G should be a group of super, polynomial growth. This insures that the number of elements in G of length n will grow faster than any polynomial in n.

Braid Groups:

Braid Groups were one of the first non-commutative groups to be suggested as a "good" suggestion as a cryptographic platform. There are many advantages and disadvantages of using braid groups in cryptography . It appears as if the conjugacy search problem in a braid group does not provide sufficient security unless keys are selected by narrow and yet to be determined subsets of the entire group.

A braid is obtained by laying down a number of parallel pieces if string and intertwining them without forgetting that they are essentially the same direction.

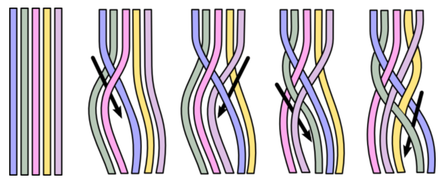


Figure 4: Five Strand Braid - Vertical direction

There are exactly $n-1$ crossing types for an n strand braid. $(x_1, ...x_{n-1}).x_i$ is a positive crossing of of the ith and i +1st strands. the set $x_1, ...x_{n-1}$ generates B_n.Each crossing is subject to the relation

$$[x_i, x_j] = 1$$

for every i, j s.t $|i-j| > 1$ and

$$x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$$

That is , the braid group B_n is denoted :

$$B_n = \left\{ x_1, ...x_{n-1} \middle| \begin{array}{c} x_i x_j x_i = x_j x_i x_j \ \ if \ \ |i-j| = 1 \\ x_i x_j = x_j x_i \ \ if \ \ |i-j| > 1 \end{array} \right\}$$

Words and Normal Groups:

- A word is any written product of group elements and their inverses. For example if $x, y, z \in G$ then $xy,\ z^{-1}xzz,\ y^{-1}zxx^{-1}yz^{-1}$ are words in the set x,y,z.Two different words may evaluate to the same value in G
- A word is called reduced if it contains no string of the form $aa^{-1}, a \in$it's generating set
- Normal form for a free group G with generating set S is a choice of a reduced word in S for each element of G

Conjugacy Search Problem (CSP):

Let G be some platform group. For example:

$$G = B_n$$

Given words $x, y \in G$ find z such that:

$$y = zxz^{-1}$$

- It has been shown that for Braid groups and other suitable platform groups this problem is undecidable.
- This means that no algorithm can be designed such that leads to the conclusion whether z exists or not and therefore offer more security potential.

Non-Abelian Cryptographic Protocols

Many different protocols exist which rely on non-abelian platform groups to perform key exchanges, encryption/decryption and authentication. These protocols aim to provide greater security than their commutative equivalents.

Anshel–Anshel–Goldfeld Key Exchange:

- Is a non-abelian alternative to the Diffie-Hellman Key Exchange.
- Requires that the platform group used has easily computable normal forms. Because of this, braid groups are primarily used as the platform group for this protocol.

Let $G = B_n$

$a = (a_1, ..., a_k),\ b = (b_1, ..., b_m) \in G$

a and b are publicly known.

Alice selects a word in a and computes its product A:

$$A = a_{i_1}^{\epsilon 1} ... a_{i_L}^{\epsilon L},\ a_{i_k} \in a,\ \epsilon_k = \pm 1$$

Bob selects a word in b and computes its product B:

$$B = b_{j_1}^{\delta 1} ... b_{j_L}^{\delta L},\ b_{j_k} \in b,\ \delta_k = \pm 1$$

Alice sends Bob the conjugates:

$$Ab_1A^{-1}, ..., Ab_mA^{-1}$$

Bob sends Alice the conjugates:

$$Ba_1B^{-1}, ..., Ba_kB^{-1}$$

Alice computes:

$$A^{-1}(Ba_{i_1}^{\epsilon 1}B^{-1})...(Ba_{i_L}^{\epsilon L}B^{-1}) = A^{-1}B^{-1}AB$$

Bob computes:

$$(Ab_{i_1}^{\epsilon 1}A^{-1})...(Ab_{i_L}^{\epsilon L}A^{-1})B = A^{-1}B^{-1}AB$$

Conclusion

Non-abelian cryptography clearly shows promise in resisting quantum computing attacks due to the CSP being undecidable for suitable platform groups. However, with their added complexity and relative lack of research they are not often implemented at present. With this said, they are one of the main candidates for the future of cryptography in the quantum computing age.

LAGRANGE'S THEOREM - A BRIEF INTRODUCTION AND HISTORY

Ryan McElhatton, Ruairi Dennehy, Enda Daly and Ross Trearty†

†National University of Ireland, Galway

Introduction to Lagrange's Theorem

This poster takes a look at mathematician Joseph Louis Lagrange, and his most famous work, 'Lagrange's Theorem'. Born in 1976, in Turin, Italy, Lagrange made huge contributions to the field of mathematics. One of his most important findings came in Group Theory where he proved a theorem that states if H is a subgroup of a finite group G, then, the size of H divides the size of G. We will take a look at Lagrange himself, his theorem, and some applications of the theorem.

Joesph Louis Lagrange

Giuseppe Luigi Lagrangia was born in Turin on the 25th of January 1736. He made for significant contributions to many areas of mathematics including analysis, number theory and mechanics. Areas in mathematics such as Lagrangian in mechanics and the Euler-Lagrange equation in calculus have been given his name as testament to his work. He passed away in Paris on the 10th of April 1813, aged 77.

The Theorem of Lagrange

Lagranges theorem states, If a function $f(x1, x2...xn)$ at $n!$ variables is acted on by all possible permutations of the variables and these permuted functions take only r distinct values then r is a division of $n!$.

Lagrange discovered this while he was trying to find an algebraic formula solution for a 5th degree polynomial and more generally for the nth degree polynomial where $n > 4$. He observed that the solution for quartic and cubic equations could be solved by finding an equation of a lower degree. These types of polynomials are known as resolvent polynomials. For this example we will write the roots as:

$$\frac{x_1x_2 + x_3x_4}{2}, \frac{x_1x_3 + x_2x_4}{2}, \frac{x_1x_4 + x_2 + x_3}{2}$$

where $x1, x2, x3, x4$ are roots of the original polynomial. In addition, he observed that all of the 4 roots are permuted in 4! = 24 ways and only these 3 values would occur. Lagrange then said that in order to solve a quintic equation, we would need a function which only takes 4 values when the variable is permuted permuted in $5! = 120$ ways.

Proof of Lagrange's Theorem

Theorem:
If *G* is a finite group of order *n* and *H* is a subgroup of G of order *k*, then k|n and $\frac{n}{k}$ is the number of distinct cosets of H in G

Proof:
To prove this theorem we start by considering the 3 lemmas outlined below.

- **Lemma 1:**If G is a group with subgroup H, then there is a one to one correspondence between H and any coset of H
- **Lemma 2:**If G is a group with subgroup H, then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 \star H = g_2 \star H$ is an equivalence relation.
- **Lemma 3:**Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then A = B.

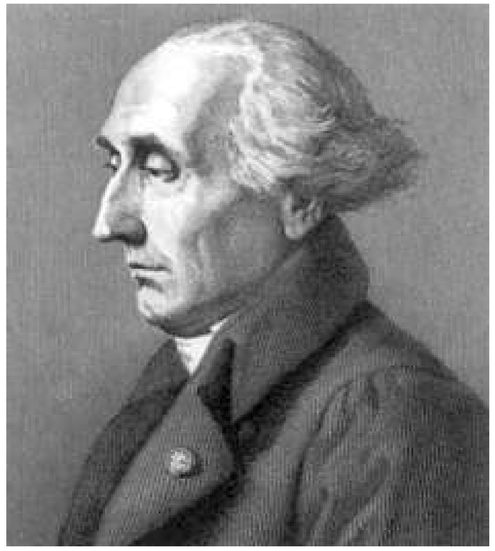


Fig. 1: Joespeh Louis Lagrange

Let $\sim$ be the left coset equivalence relation defined in Lemma 2.
It follows from Lemma 2 thatis an equivalence relation and by Lemma 3 any two distinct cosets of$\sim$are disjoint. Hence, we can write

$$G = (g_1 \star H) \cup (g_2 \star H) \cup \ldots \cup (g_n \star H)$$

where the $g_i \star$ H, i= 1,2,... are the disjoint left cosets of H guaranteed by Lemma 3. By Lemma 1, the cardinality of each of these cosets is the same as the order of H, and so

$$|G| = |g_1 \star H| + |g_2 \star H| + \ldots + |g \star H|$$
$$|G| = |H| + |H| + \ldots + |H|$$
$$|G| = n \star |H| = n \star k.$$

where k = the order of H
Q.E.D

Applications

Lagrange's theorem is often used to prove the special cases of Fermat's little theorem and its generalization, Euler's theorem, which were already known before Lagrange's theorem. Lagrange's theorem can also be used to show that there are an infinite number of primes. The theorem is also very important in the field of cryptography. With the rise of cryptocurrencies such as Bitcoin and our move towards a cashless society, work in cryptography is sure to be very important in the coming years. Bitcoin has recently reached its all time high of over 20,000 USD further proving our shift towards cryptocurrencies. Having a good knowledge of Lagrange's theorem may help you get into the world of cryptography!

Lagrange Fun Facts

Here are a few fun facts around Lagrange and his theorem

- Lagrange's interest in mathematics began by chance after reading a memoir by Edmond Halley
- In 1764, Lagrange was awarded a prize by the French Academy of Science for an essay on how apparent oscillation causes insignificant yet tangible changes in position of lunar features on the visible face of the moon. This essay included the famous equations we use today.

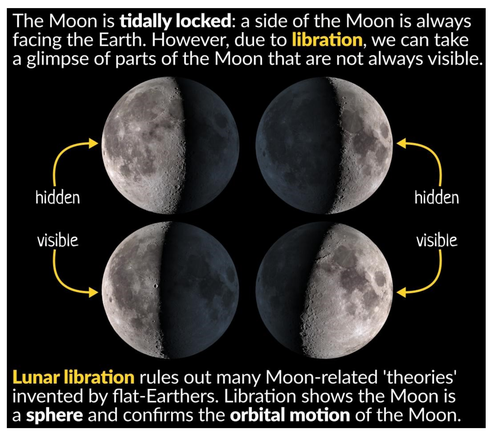


Fig. 2: The basis of one of Lagranges famous papers

- Lagrange, at Leonhard Euler's recommendation, was made Director of Mathematics at the Berlin Academy in 1766.
- Despite being both an academic, and a foreigner, Lagrange survived the French Revolution and Reign of Terror.

The Group of Symmetries of the Cube

Seán Tynan Luke Finn

Introduction

This is a poster about the group of symmetries of a cube. A cube is a 3D shape with 6 square faces, 8 vertices and 12 edges. There is a total of 48 symmetries of the cube. Comprising of 24 rotational symmetries and 24 reflections.

Reflection Symmetries

There are a total of 24 reflection symmetries of the cube and these are consisting of:

- 15 turn reflections.
- 9 plane reflections.

Turn Reflections

There are 3 axes which exists from the center of one face to the center of the opposite face and they can each be rotated 4 times. These degrees of rotation are 90°, 180° and 270° , not counting the identity. However since a 180° turn reflection is actually the antipodal symmetry, there are actually 6 turn reflections. Consisting of 3 each for the 90° and 270° rotations.

There are 4 axes which exists from a vertex to the diagonally opposing vertex and they can each be rotated 3 times. These degrees of rotation are 120° and 240°, not counting the identity. Therefore there are 8 of these turn reflections.

There are 6 axes which exists from the midpoint of one edge to the midpoint of the diagonally opposing edge and they can each be rotated twice. Again, not counting the identity, this degree of rotation is 180°. But since each of these 180° rotations are really the antipodal symmetry, there are no turn reflections for this axis either.

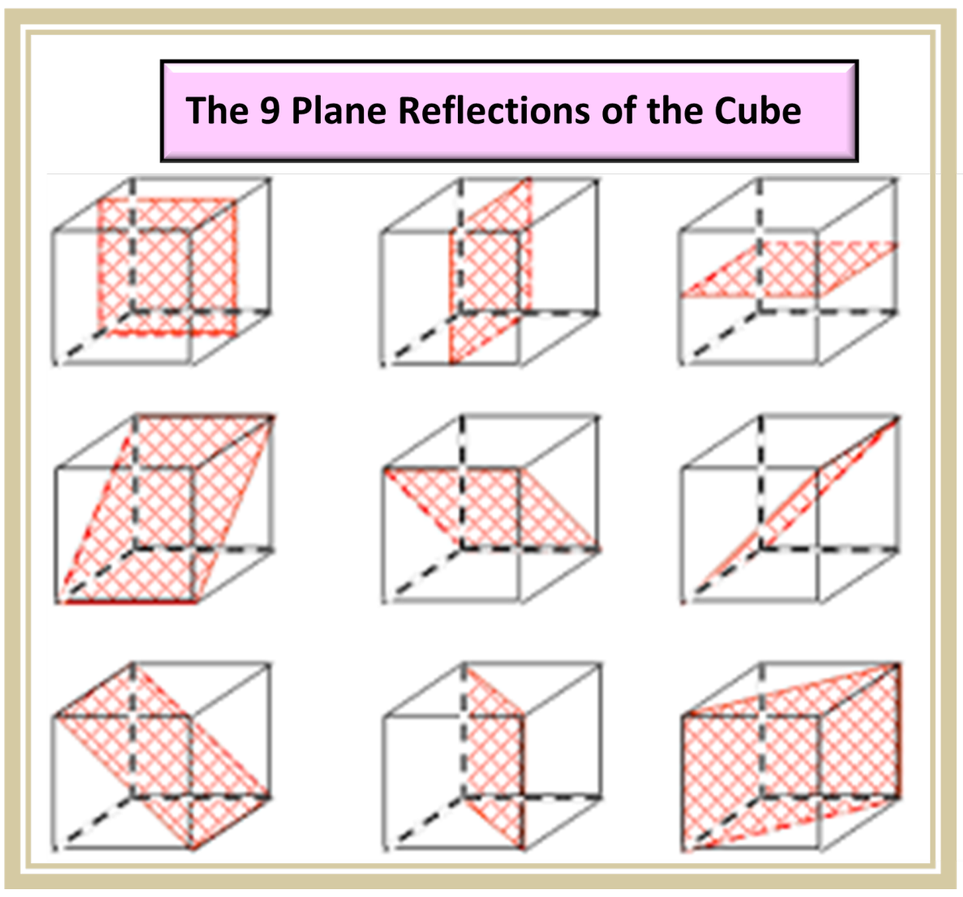
Finally we have the antipodal symmetry which was not counted in any of the above turn reflections. This is the 180° turn reflection. This is 1 turn reflection and combined with the previous 6 and 8 turn reflections stated above, brings the total to 15.

Plane Reflections

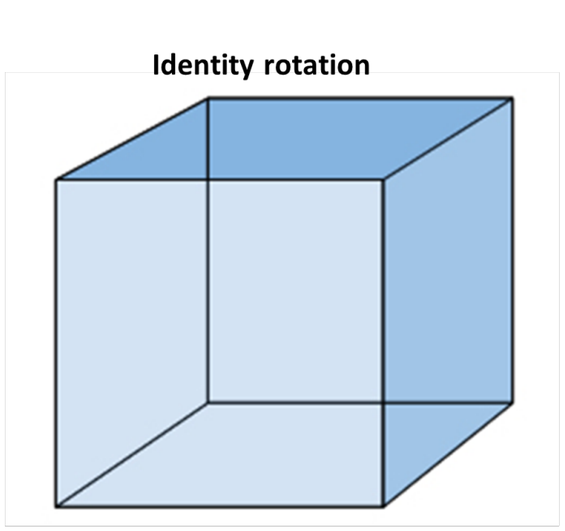
The cube has 9 reflection planes which are:

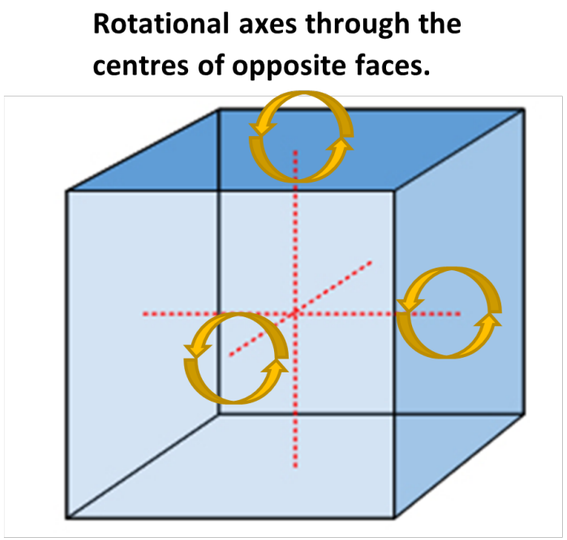
- 3 planes lie parallel to the side squares and go through the centre.
- 6 planes go through opposite edges and two body diagonals. They divide the cube into prisms.

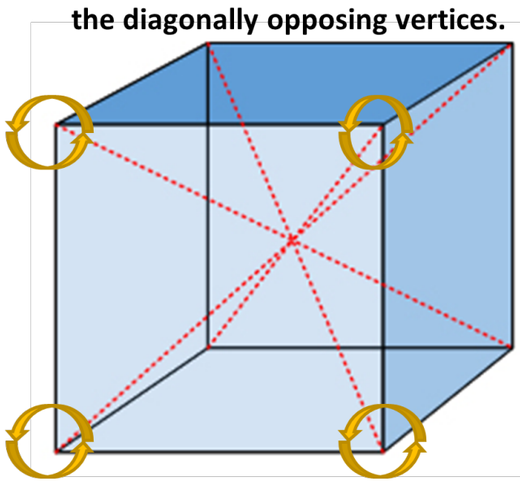
Reflection Symmetries Graphic

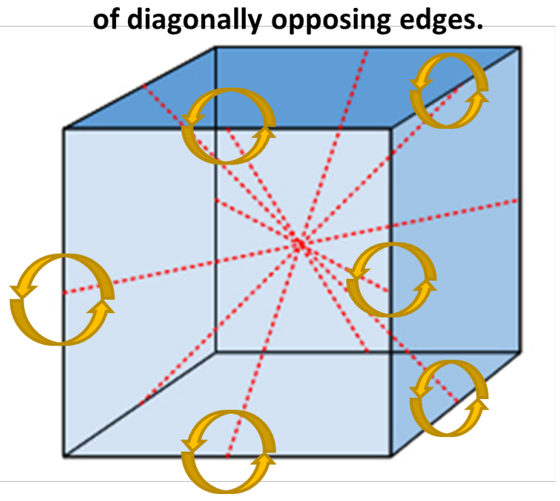


Rotation Axes Graphics









Rotational Symmetries

There is a total of 24 rotational symmetries of the cube, all of which are anti-clockwise. These consist of:

- 9 rotations about lines through the centres of opposite faces. There is a total of 3 axes of rotation, each of which has 3 rotations. Consisting of 90°, 180°, 270°.
- 8 rotations about lines through diagonally opposing vertices. There is a total of 4 axes of rotation, each of which has 2 rotations. Consisting of 120°, 240°.
- 6 rotations about lines through midpoints of diagonally opposing edges.
  There is a total of 6 axes of rotation, each of which has 1 roation. This is the rotation through 180°.
- Identity which is a rotation 0° or 360° through any of these axes.

References

Rotation images - https://i0.wp.com/peterjamesthomas.com/wp-content/uploads/2016/08/rotational-group-of-a-cube.jpg?ssl=1

Reflections - http://jwilson.coe.uga.edu/EMAT6680Fa06/Sexton/NCTMThreeDimensionalGeometry/SymmetryofaCube.html

Rubik's Cubes & Group Theory

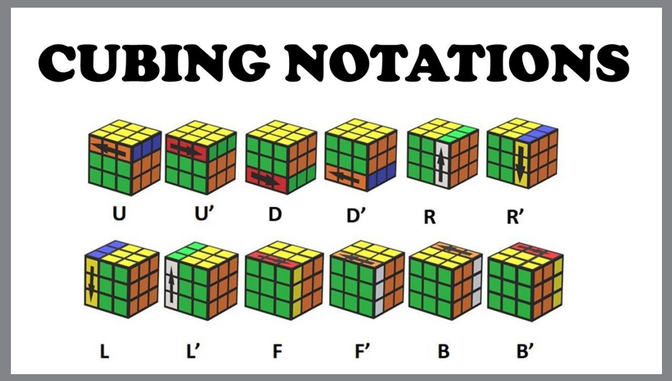
by Joshua Conneely

RUBIK'S CUBE

The Rubik's Cube is a 3-D combination puzzle invented in 1974 by Hungarian sculptor and professor of architecture Ernő Rubik. Although it reached it's peak popularity in the 1980's it is still widely know and used today.
Many "speedcubers" still use it and continue to improve on solve times.
The current world record for solving a cube is 3.47 seconds and is held by Yusheng Du.

How Group Theory and Rubik's Cube's Relate

All the possible rotations of a Rubik's Cube can be proven to be a group. First we need some notation for these rotations. Let $(R,\star)$ denote the group, where R is the set of all possible rotations, and $R_1 \star R_2$ is defined as rotating by R_1 then by R_2. Let G represent the Rubik's Cube.



U: Up, D: Down, L: Left, R: Right, F: Front, B: Back & ' is the inverse.

Proof that a Rubik's Cube is a group

Identity Element
Let R be any rotation, Let e be the Identity. Then
$e \star R = R$, $R \star e = R$
Therefore e is the Identity.

Closure
Let R_1 & $R_2 \in$ G.
For any $R_1 \star R_2$ it will produce a valid move, therefore $R_1 \star R2 \in G$. Thus is closed.

Inverse
Let R be any rotation in G, Let R' be the inverse to R. So $R \star R' = e$ and $R' \star R = e$, this shows that every rotation R has an inverse in G.

Associativity
Let R_1, R_2, $R_3 \in$ G.
$R_1 \star (R_2 \star R_3) = (R_1 \star R_2) \star R_3$
This is clearly true as for example, If you do the move $R \star (R \star U)$ its the exact same as $(R \star R) \star U$.
Therefore its associative and thus is a group.

How Group Theory Helps with Solving Rubik's Cubes

Group theory helps with solving cubes is by helping us find algorithms to solve them, as there is a very large number of permutations it is impossible to solve randomly so we need these algorithms.
These are made by looking at the commutativity of the group. The Rubik's Cube group is non-abelian ie, does not always commute
This property helps with solving them tremendously as we can devise algorithms to swap certain "cubies" (these are what the individual "cubes" are called), being able to swap these like this and not move the rest of the cubies is fundamental to solving a Rubik's cube.

Another way groups helps with solving a cube is with conjugates.
If R_1 and R_2 are two moves then the conjugate of R_1 is equal to $R_2 R_1 R'_2$
The conjugate has the same function as the original move R_1 but does the move in a different location.
This is very useful for cycling through cubies on an edge for example if you wanted to just move the top 3 corners a conjugate would be very useful here.

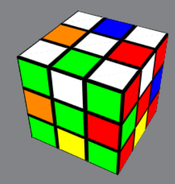
Other fact's

Number of permutations
The number of permutations possible for a Rubik's cube is a very large number.
First we need to take the 8 corner pieces so they can be arranged in 8! ways.
Then each corner piece can be arranged in 3^8 ways.
There are 12 edge pieces which can be arranged in 12! ways, then each of them has 2^{12} ways to be arranged.
But only $\frac{1}{3}$ of the permutations have the rotations of the corner cubies correct.
Only $\frac{1}{2}$ of the permutations have the same edge-flipping orientation as the original cube, and only $\frac{1}{2}$ of these have the correct cubie-rearrangement parity. So we end up with

$$\frac{(8!)(3^8)(12!)(2^{12})}{(2)(2)(3)} = 4.3x10^{19}$$

permutations.

God's Number
What is God's number, its the minimum amount of moves necessary to solve any Rubik's Cube from any state.
First we need to make a distinction between the half turn metric and the quarter turn metric.
A half turn is where any turn of 90, 180 or 270 degrees is one move Whereas a quarter turn any twist of the face is said to be a move.
God's Number is exactly 20 for the half turn metric, this was proved by Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge in 2010. It's 26 for the quarter turn metric, this was proved by Tomas Rokicki and Morley Davidson in 2014.
The superflip is the first position proven to require 20 moves (or 26 depending on which metric you prefer) the superflip is the position where all the corners are correct but all the edge pieces are flipped, the superflip actually commutes with every possible move.



School of Mathematics, Statistics and Applied Mathematics
Group Theory Poster Project
2020/2021

Frieze Groups and Mass Housing

Eoghan Breheny, Robert Deery, Ethan Goodfellow

MA3343 Group Theory Poster Project, 2020/2021

Introduction

There exists many philosophies among architects as to what constitutes good architecture. From the artistic vision down to the budget which funds it, dozens of factors are influencing what a structure will look like. With the rise of software such as autoCAD, which allows the modern architect to manipulate 2d geometry to design 3d models, a portal has been opened between what can and cannot be done with respect to exploring new ways in approaching architectural projects. Mass housing, in particular, has created a unique opportunity to combine structural design with group theory in new and interesting ways. We intend to show how group theory, in particular the application of frieze groups, can be employed to relieve the monotony of mass housing in a way that distinguishes each unit from its neighbour while maintaining the fundamental architectural properties of symmetry. This new approach towards repetitive architecture revitalises the stale aesthetics of mass housing, with methods that are precise, efficient and innovative. The thesis of this project is largely built on the work of Jin-Ho Park, as well as Alice V. James, Davd A. James, Loukas N. Kalisperis and Cornelie Leopold.

Principal Objectives

1. Introduce the concept of frieze groups.
2. Discuss the seven types of frieze groups.
3. Relate frieze groups as a solution to the issue of mass housing.

1 Frieze Groups

In design, a frieze is a pattern that regularly repeats along a given direction. Often, these friezes appear horizontally along a wall or bench. In group theory, we imagine that friezes are infinite; extending left and right. All friezes are constructed such that, if they are moved to the left or right by one unit, the overall appearance of the frieze is left unchanged. Also, there may be ways of rotating or reflecting friezes that leave its appearance unchanged. However not all friezes have this property. Each frieze belongs to a frieze group. The elements of the associated frieze group are the actions that leave the frieze's appearance unchanged. There are 5 actions that can be performed on friezes: (1) Translations r, (2) Vertical Mirror M_v, (3) Horizontal Mirror M_h, (4) Half Turn 1/2, and (5) Glide Reflections g. Using these actions we can construct the 7 standard frieze groups.

Mirrors		
Type 1:	XXXXX	*Horizontal & vertical mirrors & half turns (m_h, m_v, 1/2)*
Type 2:	VVVVV	*Vertical mirrors & half turns & glide reflections (m_v, 1/2, g)*
Type 3:	AAAAA	*Vertical mirrors & no half turn (m_v)*
Type 4:	EEEEEE	*Horizontal mirrors & no half turn (m_h)*
No Mirrors		
Type 5:	SSSSSS	*Half turns (1/2)*
Type 6:	qdqdqdq	*Glide reflections & no half turns (g)*
Type 7:	RRRRR	*Translation only*

Table 1: The seven standard frieze types.

2 Frieze Patterns in Pirgí

In 2004, a paper[1] publised by Alice V. James, Davd A. James and Loukas N. Kalisperis explored the façades of friezes in the village of Pirgí on the Greek island of Chios. The paper discovered a series of patterns which "are used to create a lively geometry, ranging from the straightforward to the complex, to give each house its distinctive identity, its own unique face to display to the world. While analyzing the frieze designs, the authors discovered that the frieze artists intuitively obey a unique set of color-reversing rules."

2.1 Notes

The paper offers three important findings: *(1)* that the geometries used in Pirgí obeyed the laws of frieze theory; *(2)* that all seven frieze types were used across the decorations of the village (see Figures 1-7); *(3)* and that frieze groups offers a unique way to establish a sense of diversity that works best when the structures are uniform and even identical.

2.2 Examples

Figure 1: Type 1, Horizontal and vertical mirrors, half turns ($m_h, m_v, 1/2$)

Figure 2: Type 2, Vertical mirrors, half turns, glide reflections ($m_v, 1/2, g$)

Figure 3: Type 3, Vertical mirrors and no half turns (bottom frieze) (m_v)

Figure 4: Type 4, Horizontal mirrors and no half turns (m_h)

Figure 5: Type 5, Half-turns and no mirrors (1/2)

Figure 6: Type 6, No mirrors, glide reflections (g)

Figure 7: Type 7, Translation only, marching right triangles

3 Modern Solutions to Modern Problems

Evidently, if you were to hold these examples up to a mathematical lens, you would undoubtedly find that these patterns are not exactly obeying the laws of group theory; this is primarily due to the fact that these façades were hand-painted and likely did not use strict measurements. However, an exact rendition of these patterns has been made infinitely easier since the conception of applications like autoCAD and ProE.

3.1 Mass Housing

As hinted in the introduction, the practice of architecture is subjective, in this project we consider the design of mass housing as the primary subject since it has more limitations (e.g. government funded, generally attached/semi-detached, relatively small units) and the crucial property of being repetitive. The fundamental application of frieze groups will be in making the façade of housing less repetitive by combining common elements in housing to subvert the generic, dissatisfying, monotonous traits typically associated with it in a cheap and efficient way.

3.2 The Work of Jin-Ho Park

In 2017, Jin-Ho Park published a paper, entitled "Subsymmetries for the Analysis and Design of Housing façades[2]," in which he sets forth an innovative approach in applying frieze groups (and combinations of their subsymmetries) to repetitive rows of housing. The application process involved using computer software to generate a 3-dimensional model of the streetscape. As mentioned already, not only does Park employ the concepts of freize theory but also introduces a "combinatorial" approach in which he combines different constituents of symmetry and subsymmetries. In his own words, "by using all or just some of the subsymmetry principles, the application results in a huge number of compositional possibilities."

3.3 Park's method

1. A series of 2-dimensional diagrams are created with respect to the frieze groups[3]. These are unique elements of the façade (not the fundamental building structure) such as doors, partial walls, windows, etc., as seen in Table 2 below:

Table 2: Seven frieze groups with design elements: a detailed example of how the complete set of frieze groups is used to design the façade

2. These elements are then *uniformly* superimposed on each other without any variation in subsymmetries in Figure 8:

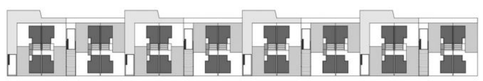


Figure 8: Final design where all elements are superimposed to form a housing façade

This creates a typical uniform housing façade. As Park notes, "Proper positioning of each symmetric element produces an orderly superimposed pattern of seven distinct symmetry operations. When overlaid together, separate building elements dissolve in a façade, having no meaning as separate rules of their juxtaposition in the entire façade, and making each underlying layer invisible."

3. Park then renders the façade elements in 3-d space, in which the underlying geometry is "not revealed," or subdued, due to its inherent asymmetrical design - offering a "dynamic look and aesthetic variety" regardless of the underlying uniform layout of subsymmetries.

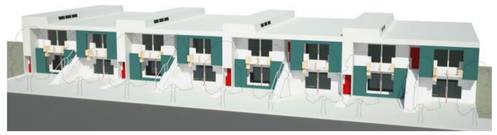


Figure 9: Three-dimensional computer model is depicted on a streetscape

4. Finally, Park begins to vary the subsymmetries of the façade: "Depending on how different parts of elements are superimposed on the façade, the expression of the final design will be different, even though it may look as if various elements are permutated, shifted, and positioned. When combined with different colors and materials, dynamic views of the alternating façades are created... In addition, a few elements may be removed, or a few subsymmetry principles left unused, thereby destroying the overall symmetry of the façade." Park presents four unique iterations[4] of the same underlying principle in Figure 10:

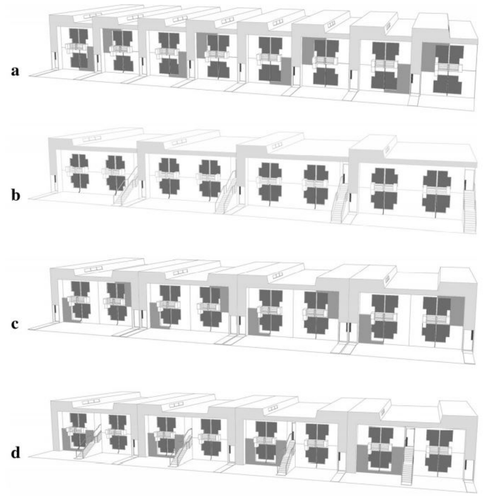


Figure 10: Four possible façade designs in that a few elements are removed or a few subsymmetry principles are not used. Although they appear similar, they are different from the ways that the principles are applied

4 Conclusion

- Group theory, and in particular the concept of frieze groups, has huge importance in structural and façade design.
- Although it has manifested in the past, modern technology now allows frieze patterns to be rendered with precision in complex and innovative ways.
- The first technological procedure for the technical application of frieze groups in architectural design was proposed (very recently) by Jin-Ho Park, whose method we have summarised and explored.
- This method can be universally applied to resolve the monotony of mass housing in a cheap, efficient way.

References

[1] A. James, D. James, L. Kalisperis, A Unique Art Form: The Friezes of Pirgi (LEONARDO, Vol. 37, No. 3, 2004) p. 235.

[2] J. Park, Subsymmetries for the Analysis and Design of Housing Facades (Nexus Network Journal, 2017).

[3] *"In Fig. 9a, the pattern is shown rooted at the successive translation of asymmetric motifs by a distance: a wall and a stair. Figure 9b portrays a pattern of flower boxes. This example illustrates where a window is translated in the line of axis and then mirrored to generate the pattern. Paired, with corner elements, windows establish a rhythm across the units. In Fig. 9c, a gutter and a lanai handrail are mirrored with a subsequent translation. Figure 9d isolates the door and aligns it along a glide reflection. Here again, a decorative lighting element is attached to remove the symmetry of the door rectangle. The motifs in Fig. 9e are paired in a half turn. This forms a partial wall boundary of a unit of row houses. Figure 9f presents a window motif in Fig. 9b that is mirrored in a half-turn and reflected in an axis line. In Fig. 9g, a wall is half-turned and reflected in two mirrors at right angles. This forms the boundary configuration of all eight row house units. All the above generates a unique pattern in forming a fac¸ade of rows of houses."* J. Park, Subsymmetries for the Analysis and Design of Housing Facades (Nexus Network Journal, 2017).

[4] *"The first model of these (Fig. 12a) is a row of houses, where each unit has a clerestory window. The exterior stair is removed and the front door for each row house is placed on the ground level. The pattern for the slightly projecting wall is also changed. In this model, the Pma2 and P1a1 subsymmetries of the frieze groups are removed. In the second model (Fig. 12b), the projecting wall pattern is removed and the exterior stair is relocated. Two units are stacked together so that the two units appear to be a single building. In this model, the Pma2 and P112 subsymmetries of the frieze groups are removed. In the third model (Fig. 12c) each unit has its own roof but the forms reflect each other horizontally. The front door is relocated and the exterior stair is removed. In this model, the P1a1 and P111 subsymmetries of the frieze groups are removed. The fourth model (Fig. 12d) removes the projecting wall of the upper floor. The roof form is reflected and the exterior stair is translated. In this model, the Pma2, P112, and P111 subsymmetries of the frieze groups are removed."* J. Park, Subsymmetries for the Analysis and Design of Housing Facades (Nexus Network Journal, 2017).

[5] C. Leopold, Geometry Concepts in Architectural Design (ReseachGate).

[6] Wikipedia (2020) Group Theory, available: *https* : *//en.wikipedia.org/wiki/Group_theory* (accessed 18 November 2020).

The Number of Generators of a Cyclic Group

Remus Ariton Emmet Connolly Cathal Byrne

MA3343

Cyclic Groups

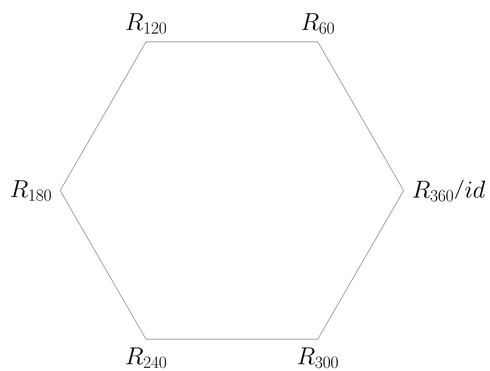


Figure 1:Rotational symmetries of D_{12}.

Let G be a group with operation $*$.
G is a cyclic group if all elements of G can be generated by a single element a and a^{-1}, where $a \in G$.
i.e G is cyclic if $G =< a >$ for some $a \in G$.
Cyclic subgroups may have more than one generating element a.

Cyclic Subgroups

A cyclic subgroup of a group can be generated by taking $x \in G$ and combining it with itself and x^{-1} to assemble a sequence of elements.

$$\ldots\ x^{-1} * x^{-1} * x^{-1},\ x^{-1} * x^{-1},\ x^{-1}, id, x, x * x,\ x * x * x \ldots$$

- A cyclic subgroup also happens to be the smallest subgroup to contain x.
- Example of a cyclic subgroup of $\mathbb{Z}$: $9\mathbb{Z}$ under the addition operator.

$$\ldots\ -36, -27, -18, -9, 0, 9, 18, 27, 36 \ldots$$

- Example of a subgroup of the dihedral group D_{12} :The rotational symmetries of D_{12} (D_{2n} where n=6 polygon). figure 1
  The group consisting of rotations by $\frac{n2\pi}{6}$ for $n = \{1, 2, \ldots, 6\}$ in the anticlockwise direction.
  The rotation $\frac{2\pi}{6}$ is an immediate example of generating element of this subgroup.

Finite Cyclic Group C_n

Elements of C_n (cyclic group with n elements) can be represented as such

$$\{x, x^2, \ldots x^n\},\ id = x^n$$

The exponent of x^{n} n indicates that x^{n} has been generated by applying x under the operation $*$ by itself $n-1$ times. e.g

$$x^3 = x * x * x$$

Generating elements of C_n from elements of C_n can be achieved by multiplication under modulus n.

$$x^i \cdot x^j = x^{(i+j)/n}$$

Where $(i+j)/n$ denotes the remainder on dividing i + j by n.
This enables us to understand which elements of C_n are generating elements of the cyclic group.

Generating Elements

Lets choose x^i as a candidate to be a generating elelment ofC_n.
Applying x^i to itself under the group operation creates elements $x^{\frac{im}{n}}$ where $m \in \mathbb{Z}$
For $x^i$to be a generating element $\frac{im}{n}$ must create the set $\{1, 2, \ldots n\}$ relating to each $x^i \in C_n$
If $x^i \in C_n$ is to generate C_n as a cyclic group i and n must be coprime in order for all elements to be produced.
Example of coprimes: 7 and 9 as they only share the factor 1.

- E.x:cyclic group $9\mathbb{Z}$ = $\{0, 1, 2, 3, \ldots, 8\}$.
  let $x^i = 2$ as 2 is coprime with 9

$$(2\cdot 0/)9 = 0, (2\cdot 1)/9 = 2, (2\cdot 2)/9 = 4, (2\cdot 3)/9 = 6, (2\cdot 4)/9 = 8, (2\cdot 5)/9 = 1$$
$$(2\cdot 6)/9 = 3, (2\cdot 7)/9 = 5, (2\cdot 8)/9 = 7,$$
$$< 2 >= \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = 9\mathbb{Z}$$

- E.x: Rotational symmetries of D_{12} = $\{R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, R_{360}\}$ id=R_{360}.
  let $x^i = x^5 = R_{300}$, clear that 5 is coprime to 6.

$*$	id	R_{300}	R^2_{300}	R^3_{300}	R^4_{300}	R^5_{300}
R_{300}	R_{300}	R_{240}	R_{180}	R_{120}	R_{60}	id

$$< R_{300} >= \{R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, R_{360}\}$$

If i and n are not coprime, $(i \cdot m)/n$ where $m \in \mathbb{Z}$ will cycle through a set containing some but not all elements of $\{1, 2, \ldots, n\}$ relating to each $x^i \in C_n$. Such x^i fail to generate all elements of C_n.

Generating Sets

x^j is an element which will generate C_n as a cyclic group, as j and n are coprime.
The order of the set of all such elements is simply Euler's totient function ϕ of n ie(the order of the set of numbers $< n$ which are co prime to n).

$$e.g : \phi(9) = |a|,\ where\ a\ is\ the\ set\ \{1, 2, 4, 5, 7, 8\}$$
$$\phi(9) = 6$$

- The generating set of the group of rotational symmetries of D_{12}.
  Order of R = $\{R_{60}, R_{120}, R_{180}, R_{240}, R_{300}, R_{360}\}$ is 6.

$$\phi(6) = |r|,\ where\ r\ is\ the\ generating\ set\ \{R_{60}, R_{300}\}$$
$$\phi(6) = 2$$

Infinite Cyclic Group

Let $< g >$ = G be an infinite cyclic group. For any infinite cyclic group G there are 2 generators. These generators are g^{-1} and g. .

Proof

If G = $< g >$ and G = $< h >$
Then g = h^n for some integer n and h = g^{mn}
G is infinitely cyclic so mn = 1
m and n are integers so they can only satisfy mn = 1 if m =1 and n=1 or (m = -1 and n = -1)
Therefore n = 1 or n = -1
Thus the only possible generators are g and g^{-1}

References

Cyclic Groups (Abstract Algebra) (2016) YouTube video, added by Socratica [Online]. Available at https://www.google.com/url?sa=tsource=webrct=jurl=https://m.youtube.com/watch%3Fv%3D8A84sA1YuPwved=2ahUKEwjKmInyvM7tAhUDqXEKHSNyCT0Qt9IBMA56BAgSEAgusg=AOvVaw2de3NB3FcXNAvyGYfmF151 [Accessed 14th of December 2020]

Unit, "An Infinite Cyclic Group has Exactly Two Generators: Is My Proof Correct?. [Accessed 13th of December 2020] https://math.stackexchange.com/questions/1075889/an-infinite-cyclic-group-has-exactly-two-generators-is-my-proof-correct ," (2014).

The Group of Symmetries of the Regular Tetrahedron

Evan O'Riordan Laura O'Donnell

Introduction to the Group of Symmetries of the Regular Tetrahedron.

This is a study of the regular tetrahedron, a three-dimensional object that consists of four vertices A, B, C, D (we could also say 1, 2, 3, 4), six edges (AB), (AC), (AD), (BC), (BD), (CD), and four faces. Four vertices give us 4! = 24 permutations or **symmetries** in this group. There are 12 rotations and 12 reflections. What are these symmetries, and what do they look like?
Note that we will be representing our symmetries using array representation, where an element on the top row is being mapped to a corresponding element on the bottom row (see examples below).

The Identity Element

In group theory, the identity element is the element of the group that when combined with any other element under the group's binary operation, regardless of the order performed, returns that other element of the group.
For the symmetries of a tetrahedron, the identity element is the transformation that leaves all the vertices in the same place. It can be thought of as not moving the tetrahedron, or else as rotating the tetrahedron 360° about any of its axes.
With array representation (vertices {A,B,C,D}), the identity element is represented as

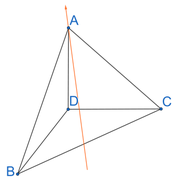
$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$$

Rotation About the Axes at the Vertices

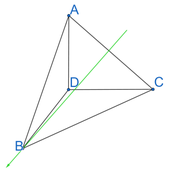
The figures below represent the four rotational axes of symmetry that connect a vertex to the center of its opposite face. For example, the axis at vertex A is the line that connects the vertex A to the center of the triangular face BCD.
Eight rotational symmetries can be found by rotating the tetrahedron by either 120° or 240° about each of these four axes. These rotations keep one vertex fixed and cycle the other three. They are as following:

	About A	About B	About C	About D
120°	$\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ D & B & A & C \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ B & D & C & A \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix}$
240°	$\begin{pmatrix} A & B & C & D \\ A & D & B & C \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ C & B & D & A \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ D & A & C & B \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ B & C & A & D \end{pmatrix}$

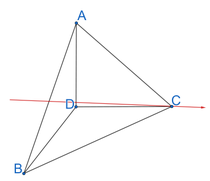
Axis at Vertex A



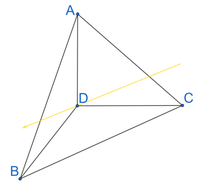
Axis at Vertex B



Axis at Vertex C



Axis at Vertex D



Rotation About the Edge Axes

Three more symmetries can be found by rotating the tetrahedron 180° along each of the axes that connect opposite edges through their midpoints, i.e. the lines connecting the midpoint of AB to CD, AC to BD, or AD to BC.
These rotations can be seen as swapping any two pairs of points. They are as follows:

AB to CD	$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$
AC to BD	$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$
AD to BC	$\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$

These rotations can also be found by composing two of the vertex rotations with opposite rotations on different vertices (e.g. 120° about A followed by 240° about B).

Reflections of Two Vertices

We can find 6 of the tetrahedrons 12 reflections by taking a pair of vertices and swapping them, while leaving the other two fixed in place. These 6 reflections are as follows:

AB	**AC**	**AD**
$\begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ D & B & C & A \end{pmatrix}$
BC	**BD**	**CD**
$\begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ A & B & D & C \end{pmatrix}$

Reflections composing of a Rotation & Reflection

The last 6 reflections can be found by combining one of the reflections with six of the rotations. We need to pick our rotations and reflections so that after composing the rotation and reflection none of the vertices are in their original position. Here are the six reflections and examples of how to find them:

(120° A) ∘ AB	**(120° B) ∘ AB**	**(240° A) ∘ AB**	**(240° B) ∘ AB**	**(AC to BD) ∘ AB**	**(AD to BC) ∘ AB**
$\begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ B & D & A & C \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ D & C & A & B \end{pmatrix}$	$\begin{pmatrix} A & B & C & D \\ C & D & B & A \end{pmatrix}$

The resulting symmetries are derangements of the four vertices. Notice how we used the reflection of AB alongside the four rotations about the vertex that kept either A or B fixed, as well as the two edge rotations that did not swap A with B. If we used any of the other rotations, at least one vertex would have stayed fixed, meaning we would not have uncovered a new reflection!

Additional Information & References

Armstrong, M. A. (1988). 'Symmetries of the Tetrahedron', *Groups and Symmetry.* New York: Springer, pp. 1-5.
Johnson, P. (2009), *Full Tetrahedral Symmetry.* viewed 6 December 2020, <http://patrickjohnson.name/311PROJ/Tetrahedron2.html>.
The figures used to represent rotations were created using Geogebra (www.geogebra.org).

LAGRANGE'S THEORM

Keyleigh Magee, Elli-Mae Maguire, Niall Carney

MA3343 Groups Poster

Introduction

In group theory, there is a well-known theorem which defines the correlation between the order of a group and the order of its subgroup. This theorem is called Lagrange's Theorem named after the Italian mathematician Joseph Louis Lagrange. This poster will explore the man himself, his theorem and its evolution into what we know Lagrange's Theorem as today.

What did Lagrange do?

Lagrange's was concerned with the question of finding an algebraic formula for the roots of the general 5_th degree polynomial and more generally for the nth (n > 4), since the quadratic, cubic and quartic formulae were already known. He observed that to solve the quartic and cubic equations involved solving supplementary polynomials of lower degree, whose coefficients were rational functions of the coefficients of the original polynomial. These polynomials are also known as "resolvent"([2]) polynomials. For this example we can write the roots as:

$$\frac{x1x2 + x3x4}{2}$$

,

$$\frac{x1x3 + x2x4}{2}$$

,

$$\frac{x1x4 + x2x3}{2}$$

where x1, x2, x3, x4 are roots of the original polynomial. Lagrange also observed that all four roots could be permuted in 4! = 24 possible ways and only these three values would occur. He then concluded: To solve 5_th degree polynomials one should try to find function in 5 variables that takes on 3(or 4) different typical values when the variables are permuted in all 5! ways.

Example: Lagrange's Theorem for C_6

We can illustrate the key ideas behind the proof of Lagrange's Theorem using the example of C_6 = (1, g, g$^2, g^3, g^4, g^5)(where g^6 = 1)$
which has as one of its subgroups H = (1, g^3).
If we multiply H on the right by each element of C_6 in turn we find the different right cosets of H in G. (1, g^3), (g, g^4), (g^2, g^5)
Using some color we can see how
H = (1, g^3)
gets "shifted" through the elements of C_6 as we multiply H on the right by elements of C_6.
C_6 = (1,g, g^2, g^3, g^4, g^5)
There are three distinct cosets.

1. Each right coset has the same size as H.
2. Two cosets are either equal or disjoint.
3. Every element of G is in exactly one right coset.

These are the key ideas needed to prove Lagrange's Theorem.

Joseph Louis Lagrange

Joseph Louis Lagrange (Giuseppe Luigi Lagrangia) was born in Turin, Italy on the 25th of January 1736. He made many contributions to several areas of mathematics, including mechanics, analysis and number theory. He is renowned in mechanics, where he reformulated Newtonian mechanics in order to simplify formulae and calculations, this is known as Lagrangian mechanics. His name is also associated with the Euler-Lagrange equation in calculus. In 1766, Lagrange moved to Berlin to pursuit mathematics after studying in the University of Turin. In 1766 he started to work on what became to be known as Lagrange's Theorem. He passed away in Paris in 1813, aged 77.

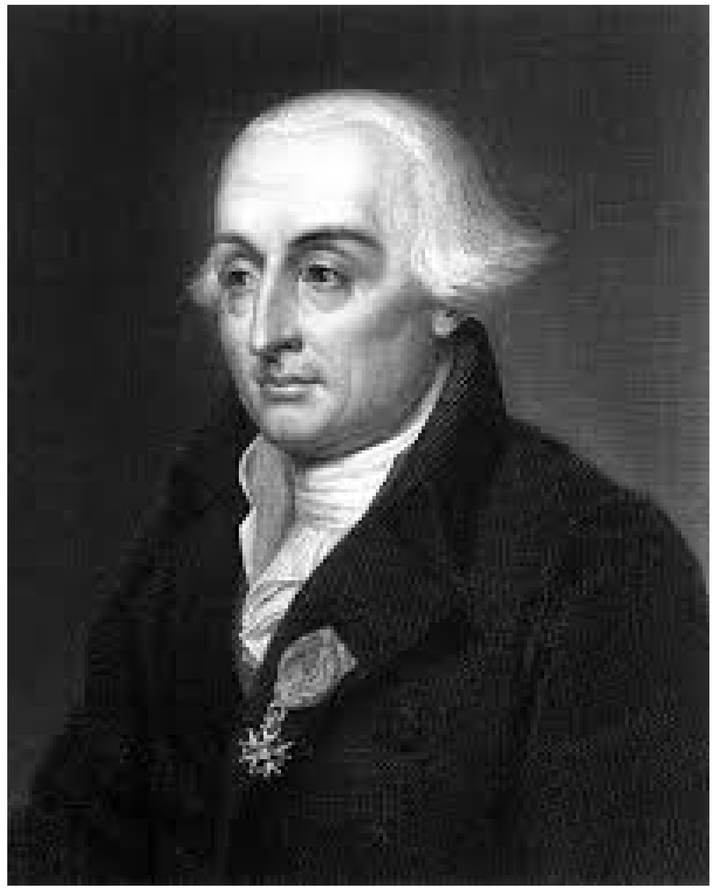


Fig. 1: joseph lagrange.jpg

Key Achievements

•Built on earlier work by Leonhard Euler to create the calculus of variations – he called it his 'method of variations.'
•Created an entirely new field of mechanics, Lagrangian mechanics, for both solids and fluids, based on the concept of virtual work and utilizing the Lagrangian function.
•Introduced the concept of generalized coordinates. Lagrangian mechanics can be used in any coordinate system – problems are simplified by choosing an appropriate one.
•Created the concept of potential: the gravitational field, for example, is a potential field.
•Discovered Lagrangian orbits.
•Solved century-old problems in number theory posed by Fermat that had defeated other mathematicians.
•Was a founder of group theory.
•Played a key role in the creation of the metric system of weights and measures.

Lagrange's Theorem

Find the subgroups that some finite group G possesses can be quite difficult. However, Lagrange's Theorem gives us more knowledge on how to find those subgroups, making the process much easier.

Theorem

If G is a finite group and H is a subgroup of G, then |H|, the order of H divides |G|, the order of G. This proves very helpful in figuring out which subgroups a group possesses provided the group is finite.For example, it tells us that a group G of order 24 cannot possibly have a subgroup of order 11.

References

Richard L. Roth. "A History of Lagrange's Theorem on Groups". In: Mathematics Magazine 74.2 (2001), pp. 99–108. ISSN: 0025570X, 19300980. URL: http://www.jstor.org/stable/2690624
Scientists, T. and Scientists, L., 2020. Joseph-Louis Lagrange - Biography, Facts And Pictures. [online] Famousscientists.org. Available at: <https://www.famousscientists.org/joseph-louis-lagrange/: :text=Joseph

The Torus of Revolution

Anton Sohn, Jack Sullivan, Sam Hudson

Investigating the translations of the surface of a torus.

The Torus of Revolution

A torus is a surface of revolution generated by revolving a circle in three-dimensional space about an axis that is coplanar with the circle. If the axis of revolution does not touch the circle, the surface has a ring shape and is called a torus of revolution. This project will explore the "translations" of the surface of a torus of revolution (which I will just call torus) as the elements of a group.

Representing Points on the Torus

Since a torus is generated by revolving a circle about the axis of revolution (AOR), which is coplanar with the circle, any point P on the torus lies on some circle that results as the intersection of the torus and the plane that contains P and the AOR.
Define the latitude $\theta \in \mathbb{R}$ of P to be the angle of the line connecting P to the centre of this circle, to some arbitrary fixed reference line through the centre of the circle.
Define the longitude $\phi \in \mathbb{R}$ of P to be the angle of the plane containing both P and the AOR, to some arbitrary fixed reference plane through the AOR.
Any point on the torus can be represented by only its longitude and latitude and no two points on the torus share the same longitude and latitude.
In summary, Every point P on the torus can be represented by a unique ordered pair $(\theta, \phi) \in \mathbb{R}^2$.

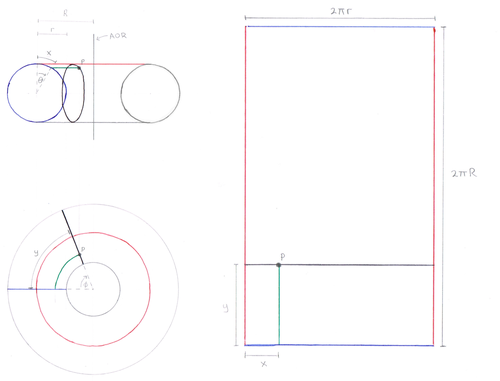


Fig. 1: Plan and Elevation of Torus and unrolled Torus

A Transformation of the Surface of the Torus

Now, we can define a transformation of the surface of the torus (which I will just call translation, although it technically is not) to be a transformation that changes the latitude and longitude of every point on the torus by two given real numbers, $\Delta\theta$ and $\Delta\phi$ respectively.
This means that every translation can be represented by an ordered pair $(\Delta\theta, \Delta\phi) \in \mathbb{R}^2$.

We can define the composition of translations $\circ$, as the sum of the ordered pairs that represent the translations. ie If the translations x and y are represented by the ordered pairs $(\Delta\theta_1, \Delta\phi_1)$ and $(\Delta\theta_2, \Delta\phi_2)$ respectively, then $x \circ y$ is represented by the ordered pair $(\Delta\theta_1+\Delta\theta_2, \Delta\phi_1+\Delta\phi_2)$. Clearly if $(\Delta\theta_1, \Delta\phi_1), (\Delta\theta_2, \Delta\phi_2) \in \mathbb{R}^2$ then $(\Delta\theta_1 + \Delta\theta_2, \Delta\phi_1 + \Delta\phi_2) \in \mathbb{R}^2$ so $x \circ y$ is also a translation. Therefore, $\circ$ is a binary operation on the set of translations.

The set of Translations as a Group

Let G be the set of all translations as defined above. Is G a group under the binary operation $\circ$?
1. Let $g_1, g_2, g_3 \in G$ where $g_i = (\Delta\theta_i, \Delta\phi_i)$ for $i = 1, 2, 3$. Then

$$(g_1 \circ g_2) \circ g_3 = (\Delta\theta_1 + \Delta\theta_2 + \Delta\theta_3, \Delta\phi_1 + \Delta\phi_2 + \Delta\phi_3) = g_1 \circ (g_2 \circ g_3)$$

2. Let $id = (0, 0)$. Clearly $id \in G$ since $(0, 0) \in \mathbb{R}^2$. Let $g = (\Delta\theta, \Delta\phi) \in G$. Then

$$g \circ id = (\Delta\theta + 0, \Delta\phi + 0) = g$$
$$id \circ g = (0 + \Delta\theta, 0 + \Delta\phi) = g$$

so there exists $id \in G$ that is the identity element for $\circ$.
3. Let $g = (\Delta\theta, \Delta\phi) \in G$. Define $g^{-1} = (-\Delta\theta, -\Delta\phi)$. Clearly, $g^{-1} \in G$ since $(-\Delta\theta, -\Delta\phi) \in \mathbb{R}^2$.

$$g \circ g^{-1} = (\Delta\theta - \Delta\theta, \Delta\phi - \Delta\phi) = (0, 0) = id$$

so every element in G has an inverse with respect to $\circ$.

$(G, \circ)$ satisfies all axioms of a group.

A Transformation of the Plane

Consider a $X \times Y$ rectangle in the Cartesian plane with one of it's vertices on the origin, one side of length X on the positive x axis, and one side of length Y on the positive y axis.
We can define a transformation of all points of the rectangle*

$$(x, y) \to (x + \Delta x \text{ [mod } X], y + \Delta y \text{ [mod } Y])$$

This is similar to a translation of all points of the rectangle $(x, y) \to (x + \Delta x, y + \Delta y)$ except that no point can be moved to a point outside of the rectangle. The transformation we have defined acts as a translation by Δx in the x direction and Δy in the y direction, but only on points that are taken to another point inside of the rectangle by said translation (ie the points (x, y) such that $0 \leq x + \Delta x < X$ and $0 \leq y + \Delta y < Y$).
However, suppose we have a point $P = (x, y)$ such that $x + \Delta x > X$. In this case the translation would move P to a point to the right of the rectangle, so our transformation takes the modulus X of the x coordinate of this translated point, such that it is between 0 and X and is thus inside the rectangle.
Visually this can be imagined as a point being moved by the transformation in the positive x direction, hitting the right side of the rectangle, jumping instantaneously to the left side of the rectangle without changing its y coordinate, and then continuing to move in the same direction (Like how Pacman can disappear from the right side of the screen and reappear on the left and vise versa).

I will refer to this type of transformation as a modular translation of the $X \times Y$ rectangle, although it is not technically a translation. Every modular translation can be represented by an ordered pair $(\Delta x, \Delta y) \in \mathbb{R}^2$.

We can define the composition of modular translations $\bullet$, as we would the composition of regular translations, as the sum of the ordered pairs that represent the translations. ie If the translations a and b are represented by the ordered pairs $(\Delta x_1, \Delta y_1)$ and $(\Delta x_2, \Delta y_2)$ respectively, then $a \bullet b$ is represented by the ordered pair $(\Delta x_1 + \Delta x_2, \Delta y_1 + \Delta y_2)$.
Let H be the set of all modular translations of a $X \times Y$ rectangle. It can be shown that H is a group under $\bullet$.

*All points of the rectangle refers to all points within the rectangle as well as one long edge and one short edge of the rectangle. The only points we exclude are one long edge and one short edge, the reason for this will hopefully become apparent later.

Unrolling the Torus

Take a $2\pi r \times 2\pi R$ rectangle where $r < R$ and roll it it up into a tube such that the two longer sides (Drawn in red in Fig. 1) of the rectangle are joined together. The radius of the tube is r and the height of the tube is $2\pi R$. All lines that were vertical grid lines on the rectangle are now circles around the circumference of the tube.
Now, we want to bend this tube into a ring such that the two circles at either end of the tube, which were once the shorter sides of the rectangle (Drawn in blue in Fig. 1), are joined together. This won't be possible without stretching the surface, so we choose the (red) line where the two longer edges of our rectangle met to remain of constant length as we bend the tube. We also ensure that the "centre" of the tube remains the same length as the original tube. It takes some thought to see that this forces the red line to be on the very "top/ bottom" of the bent tube. ie the line that, if the bent tube is placed on a table, touches the table.
Now we join the blue circles at either end of the tube together in such a way that all lines that were vertical grid lines on the rectangle, form a loop on the surface of the torus we have created. The radius of the centre of the now-bent tube, aswell as the red line (which is now a circle) is R.
The only arbitrary restrictions I have imposed on the construction of this torus is that the length of the red line and the centre of the tube remain constant.

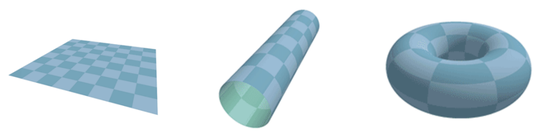


Fig. 2: Rolling a Torus

Isomorphism from H to G

Intuitively, we can see that every point on the $2\pi r \times 2\pi R$ rectangle that we started with, corresponds to some unique point on the torus. We might even suspect that every modular translation of the rectangle corresponds to exactly one translation of the surface of the torus. To show that this is true, we can find an isomorphism from H to G.
A good starting point is to realise that the Cartesian coordinates of a point P on the rectangle can be converted to our latitude-longitude coordinates of P (in radians) on the torus by the function (x,y) $\to (x/r, y/R)$. I wont go into detail, but this can be seen from fig. 1.
Now, consider a function $f : H \to G$ that takes the modular translation $h = (\Delta x, \Delta y)$ to the translation of the surface of the torus $f(h) = (\Delta x/r, \Delta y/R)$. If $h_1 = (\Delta x_1, \Delta y_1)$ and $h_2 = (\Delta x_2, \Delta y_2)$ are elements of H then

$$\begin{aligned} f(h_1 \bullet h_2) &= f(\Delta x_1 + \Delta x_2, \Delta y_1 + \Delta y_2) \\ &= ((\Delta x_1 + \Delta x_2)/r, (\Delta y_1 + \Delta y_2)/R) \\ &= (\Delta x_1/r + \Delta x_2/r, \Delta y_1/R + \Delta y_2/R) \\ &= (\Delta x_1/r, \Delta y_1/R) \circ (\Delta x_2/r, \Delta y_2/R) \\ &= f(h_1) \circ f(h_2) \end{aligned}$$

So f is a Homomorphism.
Every $g \in G$ can be written in the form $(\Delta\theta + 2n\pi, \Delta\phi + 2m\pi)$ where $n, m \in \mathbb{Z}$ and $0 \leq \Delta\theta, \Delta\phi < 2\pi$. Clearly g is the same translation as $(\Delta\theta, \Delta\phi)$ due to the periodic nature of the latitude and longitude.
Every $h \in H$ can be written in the form $(\Delta x + nX, \Delta y + mY)$ where $n, m \in \mathbb{Z}$, $0 \leq \Delta x < X$ and $0 \leq \Delta y < Y$. Clearly h is the same modular translation as $(\Delta x, \Delta y)$ due to the modular nature of the modular translation.
In summary, every $g \in G$ can be written as $(\Delta\theta, \Delta\phi)$ where $0 \leq \Delta\theta, \Delta\phi < 2\pi$ and every $h \in H$ can be written as $(\Delta x, \Delta y)$ where $0 \leq \Delta x < X$ and $0 \leq \Delta y < Y$.

Now, Let $X = 2\pi r$ and $Y = 2\pi R$. What the above tells us is that $h = (\Delta x, \Delta y)$ where $0 \leq \Delta x < 2\pi r$ and $0 \leq \Delta y < 2\pi R$ can represent any element of H.

$$\begin{aligned} f(h) = id_G = (0, 0) &\iff (\Delta x/r, \Delta y/R) = (0, 0) \\ &\iff (\Delta x, \Delta y) = (0, 0) \\ &\iff h = id_H \end{aligned}$$

so $Ker(f) = \{h \in H : f(h) = id_G\} = \{id_H\}$ which means that f is injective.

Consider $f(h) = (\Delta x/r, \Delta y/R)$. Letting $\Delta x = r\Delta\theta$ and $\Delta y = R\Delta\phi$ we get $f(h) = (\Delta\theta, \Delta\phi)$ where $0 \leq r\Delta\theta < 2\pi r$ and $0 \leq R\Delta\phi < 2\pi R$ so $0 \leq \Delta\theta, \Delta\phi < 2\pi$ since $r, R > 0$. Notice that any element of G can be written in this form. So every $g \in G$ is the image under f of some $h \in H$
so $Im(f) = \{g \in G : g = f(h) \text{ for some } h\} = G$ which means that f is surjective.
f is a both injective and surjective homomorphism, so it is an isomorphism from H to G.

Subgroups

Two of the Subgroups present within our group are

$$R_\theta = \{(\Delta\theta, 0) \in G : \Delta\theta \in \mathbb{R}\}$$

and

$$R_\phi = \{(0, \Delta\phi) \in G : \Delta\phi \in \mathbb{R}\}$$

Both of these are very unique.
$(0, \Delta\phi)$ represents the change in longitude of all points on the torus, and is known as a rotation. The torus appears to be spinning like a vinyl.
$(\Delta\theta, 0)$ is the change in latitude of all points on the torus, this one is a bit more confusing. If we imagine a torus rotating in towards its centre at a constant movement known as a revolution.

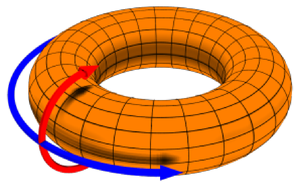


Fig. 3: Rotations (Blue Arrow) and Revolutions (Red Arrow)

Cyclic Subgroups

Let $g = (\Delta\theta, \Delta\phi) \in G$. What is the order of $\langle g \rangle$, the cyclic subgroup generated by g, and when will it be infinite?
From our definition of composition of translations, it is not hard to show that $g^n = (n\Delta\theta, n\Delta\phi)$ where $n \in F$.
So $\langle g \rangle = \{..., (-2\Delta\theta, -2\Delta\phi), (-\Delta\theta, -\Delta\phi), (0, 0), (\Delta\theta, \Delta\phi), (2\Delta\theta, 2\Delta\phi), ...\}$
We will show that if both $\Delta\theta$ and $\Delta\phi$ are rational multiples of π then the subgroup will have finite order and in any other case the subgroup will have infinite order.

Consider the elements $g_\theta, g_\phi \in G$ where $g_\theta = (\Delta\theta, 0)$ and $g_\phi = (0, \Delta\phi)$.
Let $\Delta\theta = \frac{a}{b}\pi$ where $a, b \in \mathbb{Z}$. We want to show that there exists $m \in \mathbb{Z}$ such that $g_\theta^m = (0, 0)$, ie such that $m\Delta\theta \text{ [mod } 2\pi] = 0$. Take $m = 2b$, then $m\Delta\theta \text{ [mod } 2\pi] = 2a\pi \text{ [mod } 2\pi] = 0$. So $\langle g_\theta \rangle$ has finite order. It can be shown similarly that $\langle g_\phi \rangle$ has finite order.

As with any group and an element from it, g_θ can be thought of as a permutation of the elements of $\langle g_\theta \rangle$. This permutation can be written as a single disjoint cycle $(id_G \ \ g_\theta \ \ g_\theta^2 \ ... \ g_\theta^{m-1})$ where $m = |\langle g_\theta \rangle|$. The order of this permutation is just the length of the cycle, m. Similarly, g_ϕ can be thought of as the permutation $(id_G \ g_\phi \ g_\phi^2 \ ... \ g_\phi^{n-1})$ of order n, where $n = |\langle g_\phi \rangle|$.
It can be shown that $g^k = g_\theta^k \circ g_\phi^k \quad \forall k \in \mathbb{Z}$, so $\langle g \rangle = \{id, \ g_\theta \circ g_\phi, \ g_\theta^2 \circ g_\phi^2, \ ..., \ g_\theta^{c-1} \circ g_\phi^{c-1}\}$ where $c = |\langle g \rangle|$.
As above, g can be thought of as a permutation of the elements of $\langle g \rangle$. With some thought, we see that the permutation that g represents is analogous to the product of the disjoint cycles $(id_G \ \ g_\theta \ \ g_\theta^2 \ ... \ g_\theta^{m-1})$ and $(id_G \ \ g_\phi \ \ g_\phi^2 \ ... \ g_\phi^{n-1})$. The order of the resulting permutation is the LCM of the orders of the disjoint cycles, and hence $|\langle g \rangle| = LCM(m, n)$.

Now consider $g = (\Delta\theta, \Delta\phi)$ where there does not exist $a, b \in \mathbb{Z}$ such that $\Delta\theta = \frac{a}{b}\pi$. Then $\forall a, b \in \mathbb{Z}$, $b\Delta\theta \neq a\pi$, so $\forall b \in \mathbb{Z}$, $b\Delta\theta \text{ [mod } 2\pi] \neq 0$, so $\forall b \in \mathbb{Z}$, $g^b \neq (0, 0)$, hence $\langle g \rangle$ has infinite order. It can be shown similarly that if $\Delta\phi$ is an irrational multiple of π then $\langle g \rangle$ has infinite order.

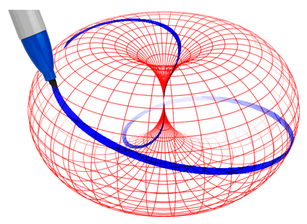


Fig. 4: Line traced by the action of a cyclic subgroup

Group Actions and Orbits

The set $S = \{(\theta, \phi) \in \mathbb{R}^2 : 0 \leq \theta, \phi < 2\pi\}$ is the set of all points on the surface of the torus. Intuitively, G acts on S, but to prove this we check two conditions;
1. $id_G \cdot s = s \ \ \forall s \in S$
Let $s = (\theta, \phi)$ then

$$id_G \cdot s = (\theta + 0, \phi + 0) = (\theta, \phi) = s$$

2. $g_1 \cdot (g_2 \dot{s}) = (g_1 \circ g_2) \cdot x \ \ \forall s \in S \ \ \forall g_1, g_2 \in G$
Let $s = (\theta, \phi)$, $g_1 = (\Delta\theta_1, \Delta\phi_1)$ and $g_2 = (\Delta\theta_2, \Delta\phi_2)$ then

$$g_1 \cdot (g_2 \cdot s) = g_1 \cdot (\theta + \Delta\theta_2, \phi + \Delta\phi_2) = (\theta + \Delta\theta_2 + \Delta\theta_1, \phi + \Delta\phi_2 + \Delta\phi_1)$$

and

$$g \circ g_2 = (\Delta\theta_1 + \Delta\theta_2, \Delta\phi_1 + \Delta\phi_2) \implies (g \circ h) \cdot s = (\theta + \Delta\theta_1 + \Delta\theta_2, \phi + \Delta\phi_1 + \Delta$$

Therefore G acts on the set S.

For some point $s_1 = (\theta_1, \phi_1) \in S$ we can translate s to any other point on the torus $s_2 = (\theta_2, \phi_2)$ by the translation $g = (\theta_2 - \theta_1, \phi_2 - \phi_1)$. So,

$$\forall s_2 \in S \ \ \exists g \in G \text{ such that } g \cdot s_1 = s_2$$

therefore $G \cdot s_1 = G \cdot s_2 = S \ \ \forall s_1, s_2 \in S$
The Orbit of any point in S under G is just S.

References

https://en.wikipedia.org/wiki/Torus
https://www.horntorus.com/illustration/standard_horntorus_turns_00.htm

THE WORLD OF ABELIAN GROUPS

Cathal Boyce and Cormac Deignan

MA3343 - December 2020

NUI Galway
OÉ Gaillimh

A look at commutativity

To discuss Abelian Groups, we first have to look at **commutativity.** When something is commutative, it means that the order in which we operate on them (this can be addition, multiplication etc.) does not affect the outcome. For example, addition over the Real numbers is commutative. It does not matter which order you add any amount of numbers in, the answer will be the same. We can also say this for multiplication.

$$a + b = b + a$$

It is important to realise that it is not the object that is being operated on that is at the root of commutativity, but it is in fact the operation itself. Note that not every operation on the Real numbers is in fact commutative, like division, for example. The root of commutativity is actually what is done to the objects (the operation) rather than what the objects are.

What is an Abelian Group?

In mathematics, an abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written. That is, the group operation is commutative.

With addition as an operation, the integers and the real numbers form abelian groups, and the concept of an abelian group may be viewed as a generalization of these examples. Abelian groups are named after early 19th century mathematician Niels Henrik Abel.

Fig. 1: Norwegian Mathematician **Niels Henrik Abel**

The concept of an abelian group is fundamental to group theory. We see it appear in many areas of the subject. One of the first visual representations we get is in the form of a multiplication table. For abelian groups, their multiplication tables are symmetric.

(Note: Abelian Groups can either be finite or infinite.)

Facts and Implications

There are certainly many implications that arise from a group being abelian. Being able to define and interpret an abelian group, whilst straightforward, can prove very useful.

1. Every subgroup of an abelian group is normal, so each subgroup gives rise to a quotient group.

2. Subgroups, quotients, and direct sums of abelian groups are abelian.

3. Every cyclic group is abelian. This is because its group operation must be commutative.

4. If a group G is abelian, the Centre of G ie. $Z(G)$ is equal to G itself.

5. If a group G is abelian (for example, all cyclic groups), then every conjugacy class in G consists of just a single element.

6.Interestingly, it is possible to find abelian subgroups of non-abelian groups. An example of this is the smallest non-abelian group, the symmetric group S_3 of order 6. All of its proper subgroups are abelian (the trivial subgroup, three subgroups of order 2 and one subgroup of order 3).

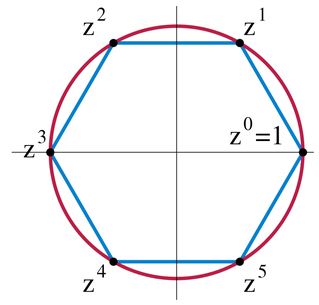


Fig. 2: Cyclic Group of 6 elements

There are also some other interesting properties relating to abelian groups. These are called "group metaproperties":

(i) Subgroup-closed group property: If G is an abelian group and H is a subgroup of G, then H is also abelian. (ie. Abelianness is subgroup-closed).

(i) Quotient-closed group property: If G is an abelian group and H is a normal subgroup of G, the quotient group G/H is also abelian. (ie. Abelianness is quotient-closed).

Examples of Abelian and Non-abelian Groups

Some abelian groups:

$(\mathbb{Z},+)$ The set of all integers under the binary operation of addition.
$(\mathbb{R}^*,\mathrm{x})$ The set of all non-negative real numbers under multiplication.

Some non-abelian groups:

$(\mathbb{Z},+)$ The set of all integers under the binary operation of addition.
$\mathrm{GL}(2,\mathbb{R})$ The set of all invertible $2x2$ matrices with real entries.

Cayley Graphs for Abelian Groups

Cayley graphs give a way of encoding information about groups in a graph. Given a group with a finite generating set, we can form a Cayley Graph for that group with respect to that generating set.

Cayley's Basic Theorem states that every group can be faithfully represented as a group of permutations. The graph below represents the graph of S_4 for all the rotations of a cube. The colours are the vertices of the RGB color cube which correspond to the numbers from 0 to 7, each number representing a vertex.

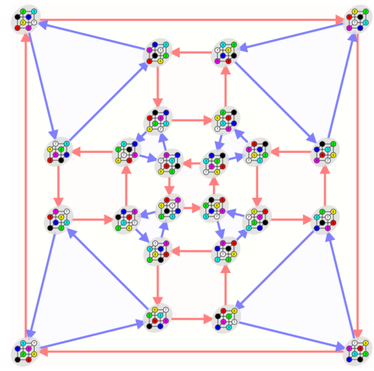


Fig. 3: Cayley graph of S_4 showing all rotations of a cube

Fundamental theorem of abelian groups

The fundamental theorem of finite abelian groups states that every finite abelian group G can be expressed as the direct sum of cyclic subgroups of prime-power order; it is also known as the basis theorem for finite abelian groups.. This is generalized by the fundamental theorem of finitely generated abelian groups, with finite groups being the special case when G has zero rank. (The rank of a group referes to the smallest cardinality of a generating set for G)

References

[1]*Lynn,Ben. (2015)* 'Abelian Groups', Stanford University. Available here: https://crypto.stanford.edu/pbc/notes/group/abelian.html

[2]*Cameron, P.J. (2004)* 'Abelian Groups', University of Oxford. Available here: http://www.maths.qmul.ac.uk/ lsoicher/designtheory.org/library/encyc/topics/abelia

[3]*Meier, J. (2008)* 'Groups, Graphs and Trees: An introduction to the Geometry of infinite groups', Cambridge Unviversity Press.

Generating Sets of Finite Symmetric Groups

Lijun Zou

Introduction

This poster serves as an after-class reading for MA3343 students. We assume the readers are familiar with the concepts of groups, generating sets, symmetric groups, cycles and transpositions. In this poster, we investigate the topic of generating sets of finite symmetric groups. In particular, we focus on the number of elements in the generating sets and find the smallest such number by mathematical reasoning.

1. S_n is generated by its all cycles

Every permutation can be written as a product of cycles, **so the set of all cycles in S_n generates S_n**. However, such set is very large and redundant. Take S_6 for example, we have $\{(1), ..., (6), (12), (13), , , , (16), (123), ...\}$, a generating set with 415 elements, and clearly not all cycles are distinct.

2. S_n is generated by its transpositions

Recall that every cycles can be written as a product of transpositions. For instance, (123) = (12)(23). Since the set of all cycles generates S_n, **the set of all transpositions is a generating set of S_n**. The total number of transpositions in S_n is $\binom{n}{2} = \frac{n(n-1)}{2}$[1]. It is a much smaller set compared the set of all cycles, but it is still redundant as (23) can be written as (12)(13)(12).

3. S_n is generated by $n-1$ transpositions

- **S_n is generated by (12)(13)(14)...(1n)**.
  Since S_n is generated by the set of all its transpositions, it is sufficient to show that an arbitrary transposition (ij) can be written as a product of transpositions containing 1[1]. Consider (1i)(1j)(1i). Element i is sent to 1 and then to j, and element j is sent to 1 and then to i. Thus, (ij) = (1i)(1j)(1i) for all $1 < i \neq j \leq n$, as required.
- **S_n is generated by (12)(23)(34)..(n-1 n)**.
  Following the above result, we only need to show that for all $1 < i \leq n$, (1i) is a product of adjacent transpositions.
  We use mathematical induction.
  •**base case** Clearly our claim holds for (12).
  •**induction step** Suppose (1i) can be written as a product of transpositions swapping 1 with other elements.
  Then (1 i+1) = (1i)(i i+1)(1i), and the result follows.
- **In both cases, we have n − 1 elements in generating sets**.

Before moving on...

We have already shown that S = $\{(12), (13), ..., (1n)\}$ is a generating set for S_n. We may ask ourselves..

Q1. **Is S non-redundant?**
A1. **YES**. If we remove any element from S, it is no longer a generating set. This is not hard to see, as removing (1i) from S leaves us a fixed point i because none of the remaining transpositions permute i. A generating set has such property is called '*Minimal*'.

Q2.**Is S the smallest generating set for S_n?**
A2. **NO**. A minimal generating set is non-redundant, but is not necessarily of the minimum size. We will see in the next section that, though S is minimal, the minimum size of generating sets for S_n where $n \geq 3$ is 2.

4. The minimum cardinality of generating sets for S_n

- S_2 is generated by (12), as (1)(2) = (12)(12) and (12) = (12).
- **For n $\geq$ 3, S_n is generated by the transposition (12) and the n-cycle (123...n)** [1].
  Since S_n is generated by (12)(23)...(n-1 n), it suffices to show that (i-1 i) where $2 \leq i \leq n$ can be generated by (12) and (123...n).
  We use mathematical induction.
  •**base case** Clearly (12) is generated by (12) and (123...n).
  •**induction step** Suppose (i-2 i-1) is generated by (12) and (123..n). We want to show (i-1 i) is also generated by these two cycles.
  For convenience, we denote (123..n) by σ.
  Consider $\sigma(i-2 \;\; i-1)\sigma^{-1}$, an element generated as requirement.
  Then, $\sigma(i-2 \;\; i-1)\sigma^{-1} = (\sigma(i-2) \;\; \sigma(i-1)) = (i-1 \;\; i)$, and the result follows.
- **For n $\geq$ 3, S_n cannot be generated by single element**.
  Recall the group generated by single elements is cyclic. Since every cyclic group is abelian, it suffices to show S_n is non-abelian.
  Let permutations $\pi_1 = (13) \in S_n$ and $\pi_2 = (12) \in S_n$.
  Then $\pi_1\pi_2 = (231)$ and $\pi_2\pi_1 = (132)$.
  It follows that S_n in non-abelian as $\pi_1\pi_2 \neq \pi_2\pi_1$.
- **Combining the above results, we conclude that the minimum cardinality of generating sets for S_n where n $\geq$ 3 is 2**.

References

Keith Conrad. *GENERATING SETS.* URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf.

Jean-Pierre Merx. *GENERATING THE SYMMETRIC GROUP WITH A TRANSPOSITION AND A MAXIMAL LENGTH CYCLE.* URL: https://www.mathcounterexamples.net/generating-the-symmetric-group-with-a-transposition-and-a-maximal-length-cycle/ (visited on 05/02/2015).

Kevin J. Mitchell. *Math 375 Week 5 5.1 Symmetric Groups.* 1999. URL: http://people.hws.edu/mitchell/math375/week05.pdf.

Rachel Quinlan. *2.3 Conjugacy in symmetric groups.* 2020. URL: http://www.maths.nuigalway.ie/~rquinlan/groups/section2-3.pdf.

The Number of Generators of a Cyclic Group

Sarah Skeffington & Griffen Small

School of Mathematics, Statistics & Applied Mathematics, National University of Ireland, Galway

1 Introduction

This poster is concerned with cyclic groups. In particular, we are interested in counting the number of elements that generate such groups and how this number depends on the order of the group. We begin with a review of cyclic groups and generators, providing examples of each. Following this, we derive an interesting formula for the number of generators of a finite cyclic group. We finish with a similar result for infinite cyclic groups.

2 Cyclic Groups and Generators

Let G be a group and let $\langle x \rangle$ be the cyclic subgroup of G generated by $x \in G$. We say that G is **cyclic** if $G = \langle x \rangle$. Equivalently, a cyclic group G is one which can be built from a single element $x \in G$ by "taking powers". Any such element x is called a **generator** for G. Every cyclic group is necessarily abelian; see [1]. We illustrate these ideas with two well-known examples.

- Let G be the group of complex 6^{th} roots of unity under multiplication

$$G = \left\{1, e^{\frac{\mathrm{i}\pi}{3}}, e^{\frac{2\mathrm{i}\pi}{3}}, e^{\mathrm{i}\pi}, e^{\frac{4\mathrm{i}\pi}{3}}, e^{\frac{5\mathrm{i}\pi}{3}}\right\}.$$

  The group is cyclic since it is generated by (for example) $x = e^{\mathrm{i}\pi/3}$; that is,

$$G = \langle x \rangle = \left\{\mathrm{id}, x, x^2, x^3, x^4, x^5\right\}, \tag{1}$$

  where $\mathrm{id} = 1$ and $x^6 = 1$. This is not the only generator for G: it is also generated by $x = e^{5\mathrm{i}\pi/3}$. It turns out that $x = e^{\mathrm{i}\pi/3}$ and $x = e^{5\mathrm{i}\pi/3}$ are the only two generators for G; see Figure 1.

- Let $G = (\mathbb{Z}, +)$ be the group of integers under addition. The group is cyclic since it is generated by (for example) $x = 1$; that is,

$$G = \langle x \rangle = \left\{\ldots, x^{-2}, x^{-1}, \mathrm{id}, x, x^2, \ldots\right\}, \tag{2}$$

  where $\mathrm{id} = 0$ and $x^n = n$. As before, this is not the only generator: $x = -1$ also generates G. It turns out that $x = 1$ and $x = -1$ are the only two generators for G.

These examples, specifically (1) and (2), demonstrate that despite superficial differences, all cyclic groups have the same abstract form. To be more precise, all cyclic groups of the same order are **isomorphic** to each other [2]. Hence we adopt a single notation $C_n = \langle x \rangle$ for all cyclic groups of order n; here it is understood that $x^n = \mathrm{id}$.

We now turn to the problem of counting the number of generators x for a given order n. First, we consider the finite case.

3 The Finite cyclic group C_n

Theorem 3.1. *Suppose that x is a generator of the finite cyclic group C_n. Then the elements of C_n that generate it as a cyclic group are exactly those elements of the form x^k, where $\gcd(k, n) = 1$. The number of these is $\phi(n)$: the Euler totient function.*

The main idea of the proof of Theorem 3.1 is to show that $C_n = \langle x^k \rangle$ if and only if $\gcd(k, n) = 1$; we say that the integers k and n are **coprime** if $\gcd(k, n) = 1$. Before giving a proof we state without proof the following result from [3]:

Lemma 3.2. *Two integers a and b are coprime if and only if there exists integers s and t such that $sa + tb = 1$.*

Proof. First, we show that $C_n = \langle x^k \rangle$ if k and n are coprime (the **sufficient condition**). By Lemma 3.2, there exists integers u and v such that $uk + vn = 1$. Then, for integral m, we have

$$\begin{aligned} x^m &= x^{m(uk+vn)} \\ &= x^{muk} x^{mvn} \\ &= (x^k)^{mu} (x^n)^{mv} \\ &= (x^k)^{mu}, \end{aligned}$$

since $x^n = \mathrm{id}$. Since the elements of C_n are exactly those of the form x^m, it follows that every element of C_n is a power of x^k, and therefore $C_n = \langle x^k \rangle$. Thus, $C_n = \langle x^k \rangle$ if k and n are coprime.

Second, we show that if $C_n = \langle x^k \rangle$, then k and n are coprime (the **necessary condition**). Since x^k generates C_n, there exists an integer u such that

$$x = (x^k)^u = x^{uk}. \tag{3}$$

Multiplying both sides of (3) by x^{-1}, we have

$$x^{uk-1} = \mathrm{id}. \tag{4}$$

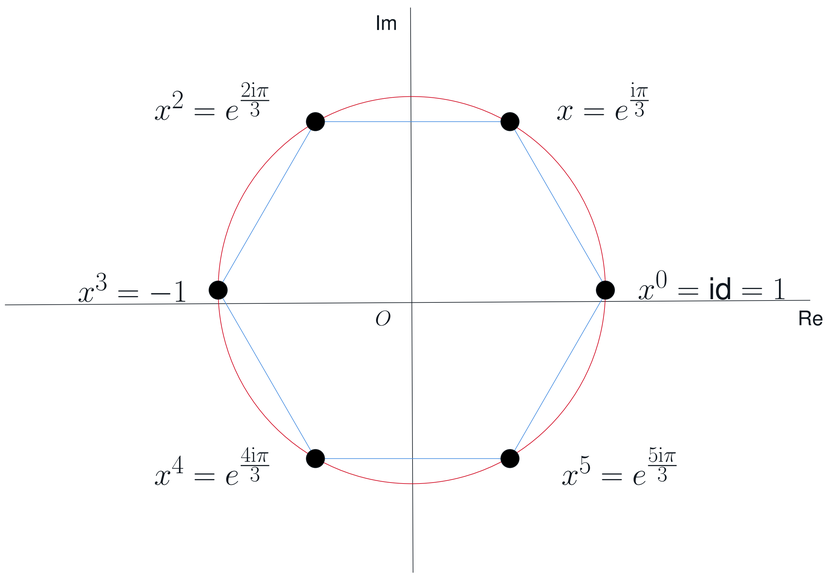


Fig. 1: The complex 6^{th} roots of unity form a cyclic group under multiplication. It is easily seen that $x = e^{\mathrm{i}\pi/3}$ and $x = e^{5\mathrm{i}\pi/3}$ are the only two generators for G .

For (4) to hold we must have that n divides $uk - 1$ (since $x^n = \mathrm{id}$). Hence there exists an integer $-v$ such that $uk - 1 = -vn$ or, equivalently, $uk + vn = 1$. It follows from Lemma 3.2 that k and n are coprime. Thus, k and n are coprime if $C_n = \langle x^k \rangle$.

We conclude that $C_n = \langle x^k \rangle$ if and only if k and n are coprime, i.e., $\gcd(k, n) = 1$. This means that $\gcd(k, n) = 1$ is a necessary and sufficient condition for x^k to generate C_n. Hence the number of distinct elements of C_n that generate it as a cyclic group is equal to the number of positive integers $k \leq n$ for which $\gcd(k, n) = 1$. The number of these is $\phi(n)$. ■

As an example, the number of distinct elements of C_6 (which we can think of as the group of complex 6^{th} roots of unity under multiplication) that generate it as a cyclic group is $\phi(6) = 2$, as claimed in § 2.

Next, we consider the infinite case.

4 The Infinite Cyclic Group C_∞

Theorem 4.1. *Suppose that x is a generator of the infinite cyclic group C_∞. Then the elements of C_∞ that generate it as a cyclic group are x and x^{-1}. So C_∞ has exactly two generators.*

Proof. First, we show that if $C_\infty = \langle x \rangle$, then $C_\infty = \langle x^{-1} \rangle$. For integral m, we have $(x^{-1})^m = x^{-m}$. Since the elements of C_∞ are exactly those of the form x^{-m}, it follows that every element of C_∞ is a power of x^{-1}, and therefore $C_\infty = \langle x^{-1} \rangle$.

Second, we show that x and x^{-1} are the only two generators for C_∞. Since $C_\infty = \langle x \rangle = \langle x^{-1} \rangle$, we must have $x = (x^{-1})^a$ for some integer a and $x^{-1} = x^b$ for some integer b. These equations imply that $x = (x^{-1})^a = x^{ab}$. Since C_∞ is infinite cyclic, $ab = 1$, and so (a, b) is either $(1, 1)$ or $(-1, -1)$. Thus, the only generators of C_∞ are x and x^{-1}. ■

We note that Theorem 4.1 is consistent with our example in § 2 of the group $(\mathbb{Z}, +)$, which had exactly two generators: $x = 1$ and $x^{-1} = -1$.

5 Remark

Theorems 3.1 and 4.1 not only yield information about the number of generators but also their form. For example, Theorem 3.1 says that the $\phi(n)$ generators for the group of complex n^{th} roots of unity under multiplication all have the from $e^{2\mathrm{i}\pi k/n}$, where $\gcd(k, n) = 1$.

6 Summary

We have shown that the finite cyclic group C_n has exactly $\phi(n)$ generators and that the infinite cyclic group C_∞ has exactly two generators. We have also illustrated these results for the case of two well-known examples of cyclic groups: the group of complex n^{th} roots of unity under multiplication and the group $(\mathbb{Z}, +)$.

7 References

[1] C. Jordan & D. Jordan. *Groups*. Newnes, 2004, p. 58.

[2] J. Rotman. *Advanced Modern Algebra*. Prentice Hall, 2003, p. 75.

[3] P. Cohn. *Algebra Volume 1*. John Wiley & Sons, 1982, pp. 27–28.

The History of Lagrange's Theorem

David O Dea, Diarmuid Donnellan, Jonathan Hester and Padraig Lafferty

NUI Galway
OÉ Gaillimh

Introduction

Our objective for this project is to examine the history of the famous Lagrange's theorem. The theorem as we know it today has evolved greatly since its earliest form in 1771. We hope to tie his initial findings about polynomials to their current applications, and the importance of the theorem to group theory and mathematics in general.

Joseph-Louis Lagrange

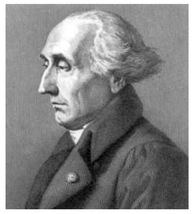


Fig. 1: Lagrange portrait

Born in Turin, Italy on 25th January 1736, Joseph-Louis Lagrange was a brilliant mathematician and astronomer. A major contributor to number theory and analysis, Lagrange also had a significant influence in celestial mechanics. His most important book, Mécanique Analytique (1788; "Analytic Mechanics"), was the basis for all later work in this field. In 1766, he succeeded Euler as the director of mathematics at the Prussian Academy of Sciences, Berlin. He moved to France in 1787 to join the French Academy of Sciences where he remained until his death in 1813. Lagrange's influence is obvious in many areas of mathematics, including theorems which carry his name either solely or jointly. Group theory had not been defined at this point in history and only began being studied in later centuries. Not having studied group theory or anything similar, Lagrange was completely unaware of the influence that his findings would subsequently have in that area of study.

Langrange's Original Findings

Lagrange initially concerned himself with finding an algebraic formula for the roots of the general 5th degree polynomial and more generally for the nth degree polynomial for n > 4. The quadratic, cubic, and quartic equations had already been solved, so Lagrange wished to investigate polynomials of degree greater than four. Lagrange observed that the solutions for the cubic and quartic equations involved solving polynomials of lower degree, or "resolvent" polynomials. "For example, the quartic was solved using using a cubic resolvent polynomial polynomial whos roots could be written as (2):

$$\frac{X1X2+X3X4}{2}, \frac{X1X3+X2X4}{2}, \frac{X1X4+X2X3}{2}$$

Where X1, X2, X3 and X4 are the roots of the original polynomial". Permute these four roots in the 4!(or 24) possible ways, and three different values are typically outputted. Lagrange reckoned a similar approach was required to solve 5th degree polynomials. He believed that a function had to be found in 5 vairables that took on 3 or 4 different typical values, where where the variables are permuted in all 5! (or 120) ways. This would lead to a corresponding resolvent that would be crucial to solving the original equation. Although Lagrange never determined if this was the case, he did however arrive at the following conclusion:
"if a function $f(X1, ..., Xn)$ of n variables is acted by n! possible permutations of the variables and these permuted functions take on only r distinct values, then r is a divisor of n!."

Timeline

Evolution of Lagranges theorem
Lagrange did not originally prove his theorem as we see it today. Although Lagrange was clearly moving towards this idea, he never in fact pinned it down. He received credit for it by many later writers.

1771
He stated that that if a polynomial in n variables has its variables permuted in all n! ways, the number of different polynomials that are obtained is always a factor of n!.

1799
Paolo Ruffini showed in 1799 that if n = 5 then m cannot be 3, 4, or 8. Inspired by Ruffini's work.

1801
Carl Friedrich Gauss proved Lagrange's theorem for the special case of (Z/pZ), the multiplicative group of nonzero integers modulo p, where p is a prime.

RÉFLEXIONS
SUR LA
RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS.

Fig. 2: Lagrange Findings 1771

1815
Augustin-Louis Cauchy showed in 1815 that if n is prime then m = 1 or m = 2 or m > n ; he conjectured that if n > 5 then m = 1 or m = 2 or m > n

1845
Joseph Bertrand proved Cauchy's conjecture in 1845 subject to the truth of his celebrated Hypothesis about prime numbers Stimulated by this, Cauchy also proved Lagrange's theorem for the symmetric group Sn.

1861
Camille Jordan finally proved Lagrange's theorem for the case of any permutation group

Langrange's Theorem As We Know It

Let G be a finite group with a subgroup H. Then the order of H divides the order of G.

Langrange's Theorem says that a subgroup of S4 which has 4! = 24 elements, could possibly have 1, 2, 3, 4, 6, 8, 12 or 24 elements, but couldn't have (for example) 11 or 17 elements.
The converse of Langrange's Theorem is not true if n and k are integers and k|n, it is not true that every group of order n has a subgroup of order k.

Proof Mechanism

Start with the subgroup H of the finite group G.
If H = G the theorem holds
If not, choose an element x of G with x ∉ H. Then the coset xH is disjoint from H and has |H| elements.
If H ∪ xH = G then |G| = 2|G| and we are done.
If not, choose y ∉ H ∪ xH and add the coset yH.
Eventually we find that G is the union of k disjoint left cosets of H, and |G| = k|H|.

Real Life Application of Lagrange's Theorem

Fig. 3: Speed Gun

There exists certain police equipment used in Italy that detects speed limit violations by motorists. It does this by snapping a pair of separate pictures of vehicles that are taken a couple of kilometres apart. If the time elapsed between the pictures is less than the time it should take to travel the distance then the vehicle is deemed to have broken the speed limit and the driver will receive a ticket. The average speed is higher than the limit. Lagrange's theorem guarantees that there existed a point on the stretch of road between the cameras where the instantaneous speed of the car was equal to the average speed, which was established by the cameras to be in excess of the speed limit.

References

1. **Newman,P., (2017): Some prehistory of Lagrange's Theorem. "The number of values of a function, https://www.m-a.org.uk/resources/downloads/3H-Peter-Neumann-Lagrange-Theorem.pdf**
2. **Roth, Richard L. "A History of Lagrange's Theorem on Groups." Mathematics Magazine, vol. 74, no. 2, 2001, pp. 99–108. JSTOR, www.jstor.org/stable/2690624.**
3. **Maths.nuigalway.ie. 2020. NUI Galway MA3343: Groups, 2020/21. [online] Available at: <http://www.maths.nuigalway.ie/ rquinlan/groups/> [Accessed 17 December 2020].**

Symmetries in Nature

Saoirse Ní Mhaoláin, Rachel Kelly, Dillon Hughes.
MA3343 Groups, NUI Galway

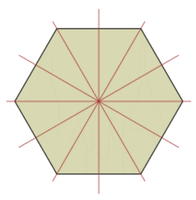
Introduction

As we observe our environment and our surroundings, we find patterns are abundant in the natural world. Patterns are visible regularities which sometimes can be modelled mathematically. From Early Greek philosophers to us now, humans studied patterns attempting to explain the order in nature. The beauty of rotational symmetry of a snowflake, the satisfying glided pattern of snake skin, the resourcefulness of the icosahedron for viruses all highlight nature's inherent propensity to form patterns. This poster attempts to link the beauty and resourcefulness of nature and mathematics in regards to symmetry.

Dihedral Groups

A dihedral group is the group of symmetries of a regular polygon, the group D2n consists of n rotations and n reflections.

There are plenty of examples of such groups in nature, the most common is the group D12 - the symmetries of a hexagon. This group has six reflections as shown below, and 6 rotations: id, R60, R120, R180, R240, R300

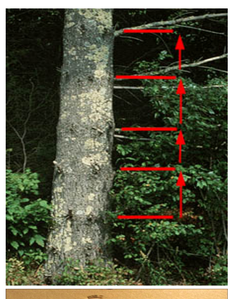


We see snowflakes have this hexagonal shape and the symmetries and rotations of D12. Honeycombs are another example, and even a close look at a dragonfly's eye shows that it is a collection of tiny lenses - all of which are hexagonal shaped. D12 is one of the many dihedral groups we can see throughout nature.

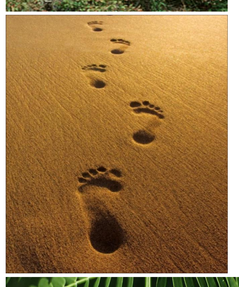
Frieze Patterns

A Frieze, or Strip Pattern contain either all or some of the following types of symmetries: Translations, Horizontal mirror reflections, Vertical mirror reflections, Rotations, Glide reflection. These symmetries form a group of seven distinct patterns: T, TR, TV, TG, TRVG, TGH and TRGHV.

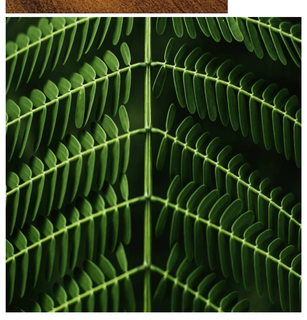
This is a picture of White Pine with some of its branches fallen off. See how each year, the tree grows new branches above each other. The white pine exhibits Translation symmetry.



Here are pictures of footprints, they are human footprints in sand. See how this forms a Translation and Glide Reflection. The right hand-side picture is a set of bear tracks. See how this is also TG symmetry.

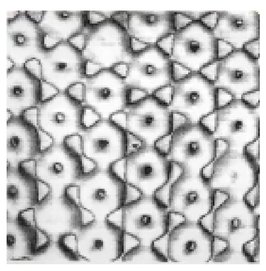


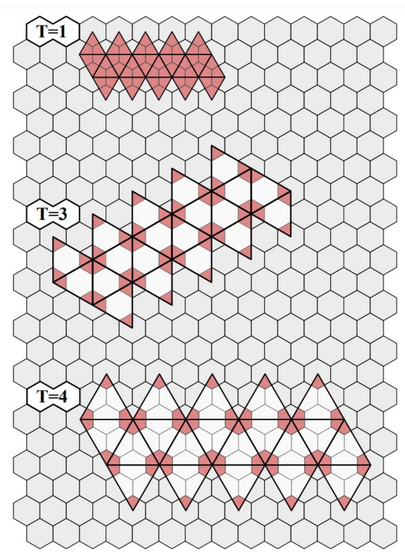
Below the footprints, is a leaf from the Mimosa tree. It displays TGH (translation and horizontal mirroring and a glide symmetry by default) symmetry.



Most snakes have TRGHV symmetry (Translation, Horizontal and Vertical Reflection and Rotation 180). This is a picture of a copperhead snake and the snake skin.

Symmetries in 3D





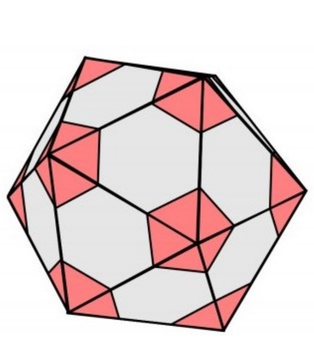
Virology

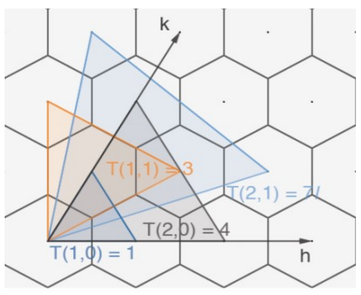
3-Dimensional objects with symmetric qualities are also evident in nature. Viruses are perhaps a surprising example of such symmetry. Viruses are protected by a protein container, called a "viral capsid". Viral capsids transport genetic material into a host, and thus hijack their hosts machinery to reproduce. For the majority of viruses, these capsids have icosahedral symmetry. It is a large group of symmetries, with order 120. 60 of these are rotations. The axes of symmetry are visible on the diagram. There is 31 in all. 15 axes through edges, 10 through the centres of faces, and 6 through vertices.

Why Icosahedrons?

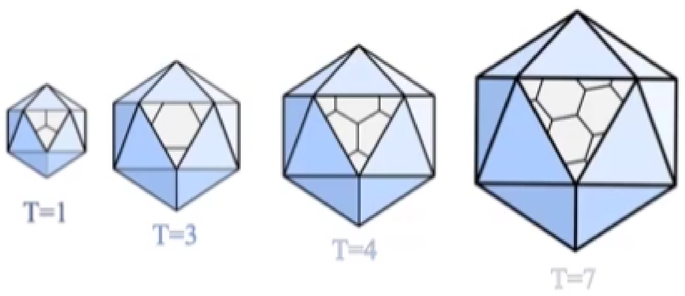
Viruses build these icosahedral capsids for reasons of genetic economy. The icosahedron consists of 20 triangular faces, and is the largest platonic solid. This makes it a relatively simple shape to produce. Viruses are extremely small, and so they have to be efficient with every piece of their genetic code. Using containers with icosahedral symmetry allows viruses to create a sufficiently large container to hold their genetic material, while minimising the amount of genetic code required.

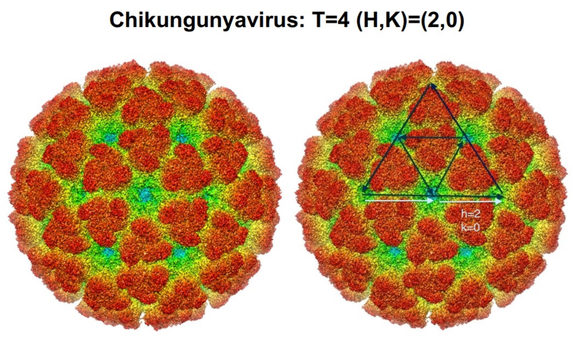
The biologists Caspar and Klug used the icosahedral nature of viruses in the 1960s to create a system known as the triangulation-number or "T-number" series. This series is used to describe different viral architectures. They were inspired by the lattice-like structure of the surface of this virus (middle left), with somewhat hexagonal groups of 6 proteins (hexamers) composing most of the shell, and groups of 5 proteins (pentamers) at the vertices. They overlayed the net of the icosahedron over a grid of hexagons, such that the vertex of each triangular face was at the centre of a hexagon. They were then able to produce many more viral capsids with different protein layouts by rescaling and rotating the net, as seen below. All of these capsids retain the symmetric properties of the icosahedron.





$$T(h,k) = h^2 + hk + k^2$$





References

Prof. Reidun Twarock - "Geometry: A New Weapon in the Fight Against Viruses" - London Mathematical Society

Finite Simple Groups and The Monster

Michael McGloin

What Are Finite Simple Groups?

Recall that a subgroup H of G is **normal** if :

$$gH = Hg \text{ for any } g \in G$$

Finite simple groups are finite groups whose only normal subgroups are the identity element and the group itself. Finite simple groups are like the "elements" of groups. Every group can be broken down into these finite simple groups by looking at so called factor groups of **composition series**

What is a Composition Series?

To understand a composition series we will first look at the definition of a subnormal series. **A subnormal series** of a group G is a sequence of subgroups of G whereby each subsequent subgroup is normal to the next one.

$$G = H_1 \trianglelefteq H_2 \trianglelefteq H_3 \ldots\ldots \trianglelefteq H_n$$

Note it is not the case that each H_i be a normal subgroup of G but only to H_{i+1}.
A subnormal series :

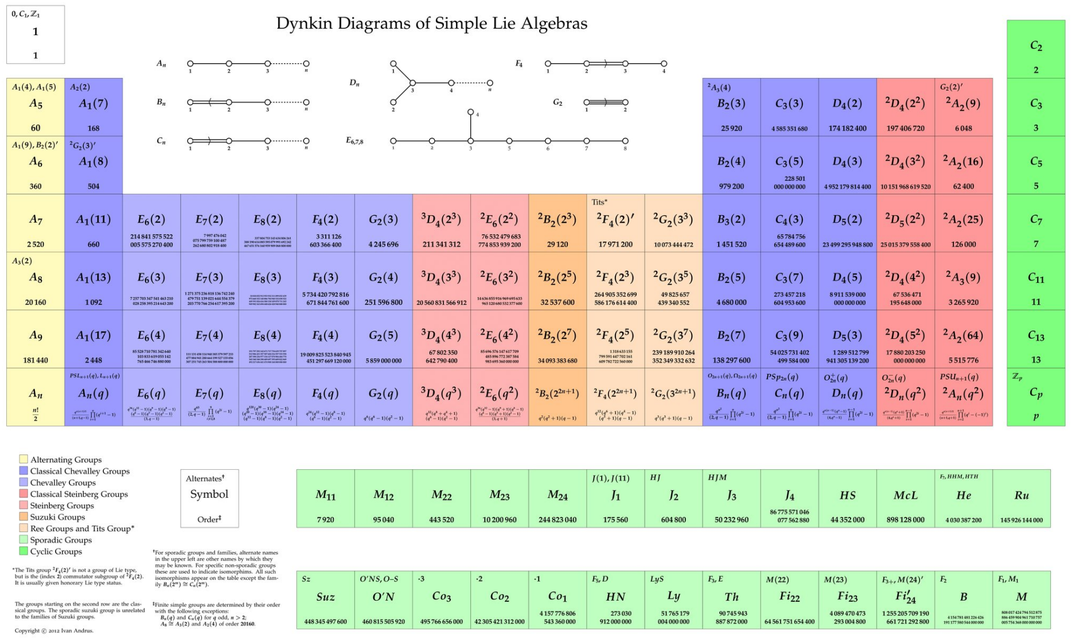
$$\{e\} = H_1 \trianglelefteq H_2 \trianglelefteq H_3 \ldots\ldots \trianglelefteq H_n = G$$

is a composition series if each factor H_{i+1}/H_i is a simple group. Every group G has a composition series.

Jordan-Hölder Theorem

Any two composition series of a group G are equivalent. Therefore every group having a composition series determines a unique list of finite simple groups and it is in this sense that the finite simple groups are the building blocks of groups !

Periodic Table of Finite Simple Groups



Every finite simple group is isomorphic to one of the groups/family of groups in the above table.

Classification of Finite Simple Groups

As it turns out there are only finitely many types of these finite simple groups. **The classification of finite simple groups** is a theorem that states that every finite simple group is isomorphic to ;
One of three infinite classes, namely :

- The cyclic groups, C_p (where p is prime)
- The alternating groups, A_n, $(n \geq 5)$
- The groups of Lie type

Or else it belongs to :

- One of the 26 sporadic groups or ,
- The Tits group (sometimes considered the 27^{th} sporadic group)

This theorem is considered to be a monumental achievement by mathematicians. No one quite knows how long exactly the proof is but it's agreed that it spans more than $10,000$ pages spread across roughly 500 journal articles by over 100 authors and was mostly published between 1955 and 2004.
The key idea for this proof came from Richard Brauer who said that you should classify the finite simple groups by finding centralizers of **involution's** (which are elements of order 2).

The Sporadic Groups

The sporadic groups are the finite simple groups that don't fit neatly into some infinite family. Some of these groups involve :

- **The Mathieu Groups** which were the first sporadic groups discovered,
- **The Conway Groups** which were discovered by John Conway by considering sphere packing in 24-dimensional space and the symmetry group of the Leech Lattice.
- **The Monster Group**, which is the largest of these groups.

The sporadic groups are divided into two different groups, **"The Happy Family"**, which are the 20 sporadic groups that can be found in the monster group and **"The Pariahs"** which are the remaining 6 that cannot be found in the monster.

The Monster

The Monster is the largest of the sporadic group. It has order 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.
It is the group of symmetries of an object that lives in 196883 dimensions (although it also has representations in higher dimensional spaces with the next one being in 21296876 dimensional space). It was predicted to exist around 1973 by Bernd Fischer but it was thought to be too enormous to be constructed at the time. However, Greiss managed to construct an algebra in 196883 dimensional space and showed that it's automorphism group was the monster.
An **automorphism** is a way of mapping some object to itself whilst preserving its structure and an **automorphism group** is simply the set of all automorphisms of an object.
This monster group would end up showing up in some rather strange places.

The J-Function

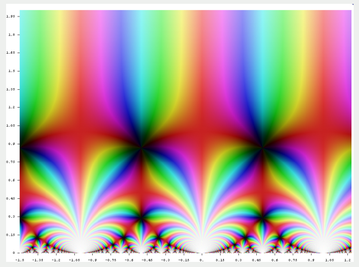
The **j-function** $J(\tau)$, a modular function discovered by Felix Klein, is the simplest function satisfying the properties :

$$J(\tau) = J(\tau + 1) = J(-1/\tau)$$

It has a power series expansion :

$$J(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots\ldots \text{ (where } q = e^{2\pi i \tau})$$

It would end up having intricate connections to the monster. Pictured on the right is the j-function in the upper-half complex plane.



Moonshine and John McKays t-shirt

When working with this j-function, John McKay noticed that the coefficient of q, **196884, was equal to 196883+1**, which is the dimension that the monster group acts on plus 1. He made a t-shirt of this fact (conceptualized on the left) and wore it to various different mathematical conferences where the general consensus was that this connection was purely coincidental.
However, it was then noticed that there were other strange connections between this j-function and the monster group. For example if you look at the coefficient of q^2, which is 21493760 in the power series expansion of the j-function, you find :

$$21493760 = 1 + 196883 + 21296876$$

which is the sum of the dimensions of the first three representations of the monster and this pattern continued for other coefficients.

Monstrous Moonshine

John Conway coined the term **"Monstrous Moonshine"** to describe this odd relationship between the monster group and the j-function and proposed the monstrous moonshine conjecture along with Simon Norton. This conjecture was proven to be true by Richard Borcherds in 1992 using many different tools such as vertex operator algebras, generalized Kac-Moody algebras and string theory in 26-dimensions.
It turned out that this connection between the monster group and these so called "modular functions" is not unique to the monster group and exists for other finite simple groups such as the Mathieu group.
This seems to have important connections with many areas of physics such as to Conformal Field Theory's and String Theory and there are many open problems related to the strange phenomenon of "moonshine".

The Number of Generators of a Cyclic Group

NUI Galway
OÉ Gaillimh

Patrick McHale Nicolas Amaya Darragh McCrann Joshua Stoney

Cyclic Groups

A cyclic group is one that is generated by a single element, in the sense that we can start with a single element and produce all the elements of G by repeatedly taking powers of that element and its inverse and by multiplying the results of such operations together.

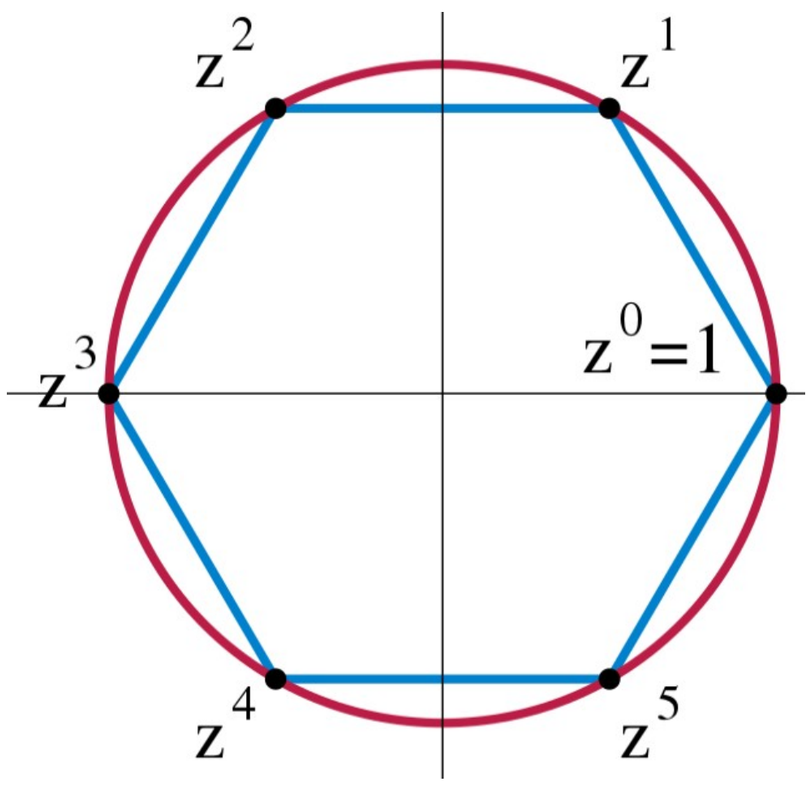
Some Examples of Cyclic Groups

- 1.) (Z, +) The integers under the operation of addition with 1 as a generator. This is an infinite cyclic group as all elements of the group can be acquired using +1 or -1. Notably the only generator in this group is +1 and -1.
- 2.) The Six 6^{th} Complex Roots of Unity with generator z^1, this forms a finite cyclic group under multiplication. See diagram below:
- 3.) $(\frac{Z}{nZ})$ The integers under addition modulo n, for every positive integer n. This is another finite cyclic group. If *i* is relatively prime to *n* then it is a generator of the group. A real-world example being musical notes of which there are 7 recurring notes A-G.

Relationship With The Number N

For a natural number n, $\phi(n)$ is the number of integers in the range 1, . . . , n that are relatively prime to n where ϕ is Euler's totient function. The number of generators of a cyclic group are relatively prime to the order of group. Every group of prime order is cyclic.
We can see this in the example below.
For example 12(which is Z12=(0,1,2,3,4,5,6,7,8,9,10,11)).
⟨0⟩= (0)
⟨1⟩= (1,2,3,4,5,6,7,8,9,10,11,0)= Z12
⟨2⟩= (2,4,6,8,10,0)
⟨3⟩= (3,6,9,0)
⟨4⟩=(0,4,8)
⟨5⟩= Z12
⟨6⟩= (0,6)
⟨7⟩= Z12
⟨8⟩= (8,4,0)
⟨9⟩= (9,6,3,0)
⟨10⟩= (10,8,6,4,2,0)
⟨11⟩= Z12
If its relatively prime to 12 it generates Z12. This illustrates that all generators in a cyclic group are relatively prime to that group's order.

The Six 6^{th} Complex Roots of Unity



Finite Cyclic Groups

A finite cyclic group is a group that has a finite cardinality, is cyclic and is isomorphic to the integers modulo *n* for some positive integer. If G is a cyclic group with a finite order *n* and a generator *a*, then G is isomorphic to $(Z_n, +)$. In other words, every finite cyclic subgroup is isomorphic to $(\frac{Z}{nZ})$, the integers mod *n*.
If G is finite, of order *n*, the group generated by g is denoted $\langle g \rangle$. The order of a finite cyclic group is the number of elements in the group, aka the cardinality of the group.
If the cyclic subgroup $\langle a \rangle$ of G is finite then the order of *a* is the order of the cyclic group.
Every finitely generated abelian group is a direct product of cyclic groups.

The Number of Generators in an Infinite Set

Let $G = \langle a \rangle$ be an infinite cyclic group.
Since a is the generator of G then a^{-1} is also a generator of G (as G is a group)
Let b be any generator of G. Then *b* and $G = \langle a \rangle$
$\rightarrow b = a^n$ for some n
For *a* and $G = \langle b \rangle$
$\rightarrow a = b^m$ for some m
$\rightarrow a = b^m = (a^n)^m = a^{nm}$
$\rightarrow$ nm=1 $\rightarrow m = \frac{1}{n} \rightarrow n = \pm 1 \rightarrow$ b= a or a^{-1}
$\therefore$ An infinite cyclic group, has precisely 2 generators

References

- https://www.youtube.com/watch?v=BipvGD-LCjU
- https://laurensommers.files.wordpress.com/2014/12/capstonefinal2.pdf?fbclid=IwAR0eYAS1o9qjx4FXIIw2CcZKjL0_cBWcjgoNOQSlvEL0jkBo82w6pFCLTe8
- https://en.wikipedia.org/wiki/Cyclic_group#Integer_and_modular_addition
- Quinlan, R., 2020. Groups sections 1-3
- https://mathworld.wolfram.com/CyclicGroup.html

Group Theory in Music: Neo-Riemannian Theory

Adam McDonagh
17323313

OÉ Gaillimh
NUI Galway

The Musical Space

'Music is not only a mysterious and metaphorical art; it is born of science ...it is made of mathematically measurable elements ...any explanation of music must combine mathematics with aesthetics' [3]

Group theory can be applied to the basics of music theory as a means of enriching our understanding of the machinery of musical operations, and also as a means of highlighting the real-life applications of this branch of mathematics. Firstly, however, we must address the concept of the musical space.

Assuming octave equivalence (i.e. a given C note is equivalent to all C notes in higher and lower octaves) and enharmonic equivalence (i.e. $C\sharp = D\flat$) we can assign an integer modulo 12 to every note in the musical space as in Fig.1 below.

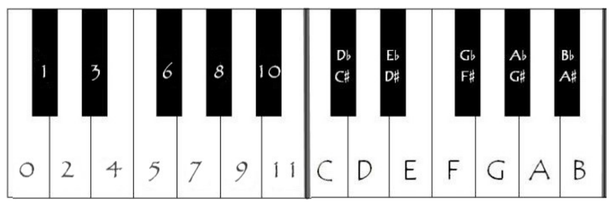


Fig. 1: Pitch-Class Integers [5]

We can then think of the interval between any two notes a, b as

$$a - b \mod 12$$

Furthermore, each major and minor chord can be represented by a pitch-class set consisting of the three pitch-class integers that form the triad. For example, a C major triad is denoted by (0,4,7).

Transpositions as Cyclic Groups

A transposition $T_n(x)$ in the musical space moves a pitch $x \in \mathbb{Z}_{12}$ up by $n \mod 12$. If we take $T_7(x)$ to be the transposition that moves each x up by $7 \mod 12$, we can generate the entire group of all such transpositions [4].

$$< T_7 >= \{T_7, T_2, T_9, T_4, T_{11}, T_6, T_1, T_8, T_3, T_{10}, T_5, T_0\}$$

This represents a circle of fifths starting at the pitch-class x. If $x = 0$, the pitch-class of C, then:

$$< T_7(C) >= \{G, D, A, E, B, F\sharp, C\sharp, G\sharp, E\flat, B\flat, F, C\}$$

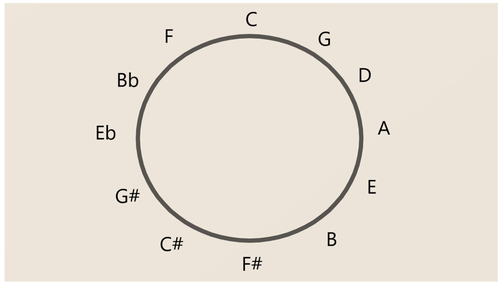


Fig. 2: Circle of Fifths generated by $T_7(x)$

Inversions & the TI Group

It is worth noting that the group of transpositions mentioned earlier can be applied to single notes, triads or to melodic phrases. If we define an inversion I_n of a triad $x = (a, b, c)$ as

$$I_n = -x + n = (-a + n, -b + n, -c + n)$$

and then form the set of all transpositions and inversions, defined as

$$TI = \{T_n, I_n : n = 0, ..., 11\}.$$

It is shown in [2] that TI is a group under composition:

1. Composition of functions is always associative by definition.
2. It can be shown that TI is closed by considering

$$T_m \circ T_n = T_{m+n} \mod 12$$
$$T_m \circ I_n = I_{m+n} \mod 12$$
$$I_m \circ T_n = I_{m-n} \mod 12$$
$$I_m \circ I_n = T_{m-n} \mod 12$$

3. Note that $id_{TI} = T_0$ as

$$T_0 \circ T_n = Tn = T_n \circ T_0$$
$$I_n \circ T_0 = I_n = T_0 \circ I_n$$

4. By the equations in 2, the inverse of each T_n is T_{12-n} and the inverse of each I_n is itself.

PLR Group

Although the TI group can be useful in terms of showing that we can get from any triad to another simply by applying transpositions and inversions, the TI group falls short in its musical practicality. As well as possessing a practical musical description, the set of PLR transformations as defined below also has a strong connection with group theory. The PLR group forms a key part of Neo-Riemannian theory, put forward initially by David Lewin and based largely on the work of Hugo Riemann. Each of the PLR operations can be defined as follows:

P: The parallel operation P sends a triad to its unique triad of opposite parity. For example, P sends C major=(0,4,7) to C minor=(0, 3, 7) and vice versa.

L: The leading-tone exchange operation L shifts the bottom note of a major triad down by a semitone and shifts the top note of a minor triad up by a semitone.

$$L(Cmajor) = L(0, 4, 7) = (11, 4, 7) = Eminor$$
$$L(Cminor) = L(0, 3, 7) = (0, 3, 8) = A\flat major$$

R: The relative operation R sends a major triad to its relative minor by shifting the top note of the triad up a whole tone (up by 2). Conversely, R sends a minor triad to its relative major by shifting the bottom note down by a whole tone.

$$R(Cmajor) = R(0, 4, 7) = (0, 4, 9) = Aminor$$
$$R(Cminor) = R(0, 3, 7) = (10, 3, 7) = E\flat major$$

It is woth noting that P, L, R are involutive:

$$P^2 = L^2 = R^2 = id$$

PLR Group = D_{24}

It is proved in [2] that the set of all PLR transformations forms a group under composition. It can also be shown that this PLR group is equivalent to D_{24}, the dihedral group of order 24.

D_{24} is generated by a rotation r and a refelction s such that

$$s^2 = r^{12} = id_{D_{24}}$$
$$srs = r^{-1}$$

We can see that the PLR group consists of 24 distinct bijections and that the group has order of at least 24, by alternately applying R and L to the C major triad:

$$C, a, F, d, B, g, E, c, A, f, D, b, G, e, B, g, E, c, A, f, D, b, G, e, C$$

where capital letters represent major triads and lower case letters represent minor triads. Note that $R(LR)^3 = P$, which tells us that the PLR group can be generated by L and R.

Now let $r = LR$ and $s = L$. Then $r^{12} = id = s^2$ and

$$srs = L(LR)L = RL = s^{-1}$$

Finally, [1] shows that the PLR group has exactly 24 elements by showing it is a subgroup of the aforementioned TI group which has order 24.

The Tonnetz

The *Tonnetz*, or tone network, can be used as a geometric representation of the PLR transformations. Since Euler first intouduced it, the tonnetz has been developed by Hugo Riemann and David Lewin, among others. As the tonnetz in Fig.3 is expanded, it repeats and can be then projected onto a torus. Note that each triangle in Fig.3 represents a major or minor triad which together, triangulate the torus. Also, since each PLR action only alters one note, these actions can be considered as reflections of triangles about one of its edges.

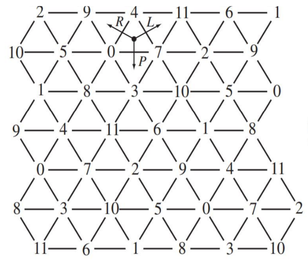


Fig. 3: Tonnetz [2]

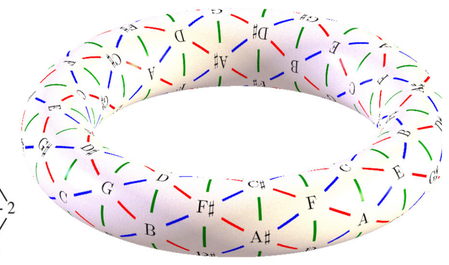


Fig. 4: Tonnetz lying on a torus

References

[1] Alissa S. Crans et al. "Musical Actions of Dihedral Groups". In: *American Mathematical Monthly* 116 (2007), pp. 479–495.

[2] F. Aceff-Sánchez et al. *An Introduction to Group Theory with applications to Mathematical Music Theory*. Publicaciones Electrónicas Sociedad Matemática Mexicana, 2012.

[3] L. Bernstein. *The Unanswered Question*. Harvard University Press, 1976.

[4] E.B. Roon. *That strikes a chord! An illustration of permutation groups in music theory*. 2019.

[5] A. Zhang. *The Framework of Music Theory as Represented with Groups*.

Groups of integers modulo n

Orlaith Ní Chonaire Jan Kruszyński

Introduction

A group G is a set equipped with a binary operation that combines any two elements to form a third element in such a way that four conditions called group axioms are satisfied, namely closure, associativity, identity and invertibility.

This poster is designed to expand the reader's understanding of Group Theory.

Unit Groups modulo n

$\mathbb{Z}_n$, a unit group of integers modulo n is the set, of n non-negative elements, represented by

$$\{0, 1, \ldots, n - 1\}$$

with addition and multiplication modulo n. Elements of this set do not form a group under multiplication since 0 does not have a multiplicative inverse.[1]

Lagrange's Theorem:

states that in group theory, for any finite group say G, the order of subgroup H of group G divides the order of G. The order of the group represents the number of elements. We can use Lagrange's Theorem to make it a lot easier to find a subgroup of the group of units in .

We can prove this by supposing H is a finite subgroup of a group G and that $g \in G$. Then gH has the same number of elements as H.

We write k for the order of H and write $\{h_1, h_2, ..., h_k\}$ for the elements of H to prove this. Meaning the elements of gH will be $gh_1, gh_2, ..., gh_k$. This shows that gH has k elements, to prove this we just have to prove that there is no repetition in this list.

So suppose that $ghi = ghj$ for some i and j in the range $\{1, ..., k\}$.

We can multiply both sides of this equation on the left by g^{-1} to deduce that this means $hi = hj$ and therefore $i = j$.

So ghi are distinct for $i = \{1, ..., k\}$ and the coset gH has the same number of elements as H. [3]

To Prove Un is a Group Under Multiplication

This is done by supposing Un is the set of units in Zn , $n \geqslant 1$ with a, b $\in$ *U*n, *where*

a having multiplicative inverse a^{-1} *and*,

b having multiplicative inverse b^{-1}

we see,

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(1)b = b^{-1}b = 1$$
$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1$$

Showing that the identity element for multiplication mod n is 1, where $n \geqslant 1$ is a unit in $\mathbb{Z}$, 1 with a unit in $\mathbb{Z}_n$ with multiplicative inverse 1, meaning every element of Un has a multiplicative inverse.[2]

Example: U_8 Multiplication

$\mathbb{Z}_n$ is a group under multiplication modulo n if and only if its elements are relatively prime. Groups of units in $\mathbb{Z}_8$: there are four elements within $\mathbb{Z}_8$ that are coprime to 8

$$U_8 = \{1, 3, 5, 7\}$$

We'll multiply elements of U_8 and the reduce the outcome by mod 8.

For any $\mathbb{Z}_n$ where n is larger than 0, and if n is divisible by 2 we can easily find out how many elements are coprime to n from the equation $\frac{n}{2}$.

U_8, *Multiplication*				
x	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

References

Hans Reisel Carl Friedrich Gauss Arthur Clarke. "Multiplicative group of integers modulo n". In: (2020).

Bruce Ikenaga. "The Group of Units in the Integers mod n". In: 1 (2018), pp. 1–4.

Rachel Quinlan. "Essential concepts of group theory". In: (recentl years), pp. 15–18.

Rotational Symmetries Of A Cube

John Tierney, James Foley, Darragh Flannery, Colm Og Conneely

National University of Ireland, Galway

Overview

We will look at the following aspects of the Group of Rotational Symmetries of a Cube.

- Showing that the rotations of a cube form a group.
- Illustrating the various rotations and axes of the rotations of a cube.
- Proving the group obeys the orbit stabilizer theorem.
- Showing the group of rotations of a cube is isomorphic to S_4

Prove that the Rotations of a Cube form a Group

Here G is the set of rotations of a cube and let x be some arbitrary rotation of the cube, i.e x in G.

- Identity
  We need to show that there is an element id such that id * x = x * id = x for x in G. we need any rotation which leaves the cube completely unchanged. The rotation by 360 degrees through any axis does this, so id in G
- Closure
  Let a, b in G. Must show a * b in G. Apply a to an unmarked cube simply rotates the cube about a certain axis, leaving a seemingly identical cube. Applying b then after this leaves an identical cube as well. So a * b in G
- Inverse
  Each rotation is the inverse of itself. If you apply rotation x to a cube in one direction and then rotate in the opposite direction by the same degree, you are left with the cube you started with. This is true for any rotation x in G. Thus inverse of x is in G.

Isomorphism to S_4

The group of rotations of a cube has the same order as S_4, 24. We need to show the group is isomorphic to a subgroup of S_4. Remark that a cube has four diagonals and that the rotation group induces a group of permutations on the four diagonals. However we must not assume that different rotations correspond to different permutations.
Now labelling the consecutive diagonals 1,2,3 and 4, we see two perpendicular axes where 90 degree rotations give the permutations $alpha = (1234)$ and $alpha = (1432)$. These induce an 8 element subgroup and a 3 element subgroup $\{id, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\}, \{id, \alpha\beta, (\alpha\beta)^2\}$ respectively. Therefore, the rotations induce all 24 permutations since $24 = lcm(8, 3)$ [2].

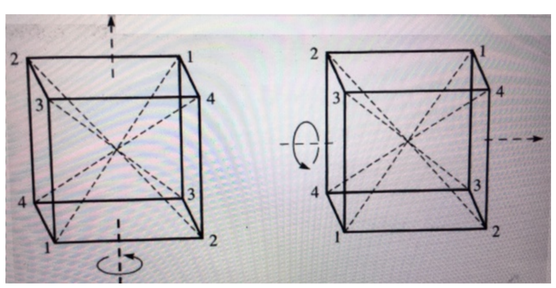


Fig. 1: $\alpha = (1, 2, 3, 4)\beta = (1, 4, 3, 2)$

Rotations and Axes of Rotation

The cube has a total of 24 rotations. The first rotation is the identity Now lets look at the diagram below on the left. We have nine rotations, we can rotate by $90°, 180°$, or $270°$, around each of the three axes shown. Each of these nine rotations will leave two faces fixed, and all vertices and edges are not fixed.The middle diagram shows six more rotations of the cube. These six leave two edges fixed, while no faces or vertices are fixed. The final diagram below shows rotations around the axes made by joining opposite vertices, we can rotate by $120°, 240°$ about these four axes, resulting in eight more rotations.

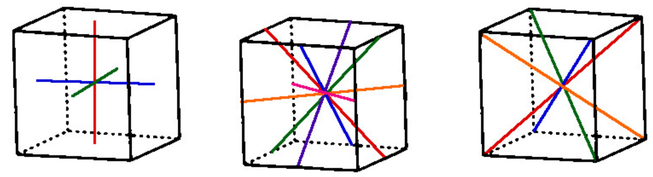


Fig. 2: Rotational Axis of a cube

[1]

The Orbit-Stabilizer Theorem

We let f = a face in a cube
|G . f] = |G : Stab$_G$(f)|
(Aside: We note that there are 24 rotational symmetries in a cube i.e. |G| = 24)

Proof:
If we take any face on a cube, it is possible to move from that face to any other face in the cube (as seen in the first figure above).We then have that the orbit of any face is $\{1, 2, 3, 4, 5, 6\}$ (the numbers 1 to 6 represent a face on the cube).The stabilizer of all faces in a cube are $\{id, R_{90}, R_{180}, R_{270}\}$ (as seen in the first image (left) above and we then apply the appropriate axis in each case).
|G . f| = 6, |G : Stab$_G$(f)| = |24 : 4| = 6
6 = 6

We now take a look at the edges.
We let e = an edge in a cube
|G . e] = |G : Stab$_G$(e)|
(Aside: Again we note that there are 24 rotational symmetries in a cube i.e. |G| = 24)

Proof:
If we take any edge on a cube, it is possible to move from that edge to any other edge in the cube. So, we then have that the orbit of any edge is $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ (the numbers 1 to 12 represent an edge on the cube). The stabilizer of any edge on the cube is $\{id, R_{180}\}$ (where the axis of rotation goes from the centre of that edge to the centre of the edge on the face directly opposite to it, passing through the centre of the cube, as seen in the middle image above.
|G . e| = 12, |G : Stab$_G$(e)| = |24 : 2| = 12
12 = 12

Subgroups

We now take a look at the subgroups of the rotational symmetries of a cube.

- The stabilizer of each face forms a subgroup of order 4 and the stabilizer of each edge forms a subgroup of order 2.
- If we examine the first image (left) as seen under Rotations and Axis of Rotation, which shows the face midpoint rotations.For the axes shown, all rotations through the same axis form a subgroup of order 4.
- We now examine the middle image as seen under Rotations and Axis of Rotation, which shows the edge midpoint rotations. For the axes shown, all rotations through the same axis form a subgroup of order 2.
- Lastly, we examine the last image (right) as seen under Rotations and Axis of Rotation, which shows the diagonal rotations. For the axes shown, all rotations through the same axis form a subgroup of order 3.

The order of the subgroups are 2,3 and 4, which are factors of |G| = 24. This verifies Lagrange's theorem.

Is the Group Abelian?

Centre of the group, $Z(G) = \{id\}$, the centralizer of any element x of the group $C_G(x) =$ {id, any rotation on the same axis as that rotation x}. Hence the group is not abelian as not every element of the group commutes with one another.

References

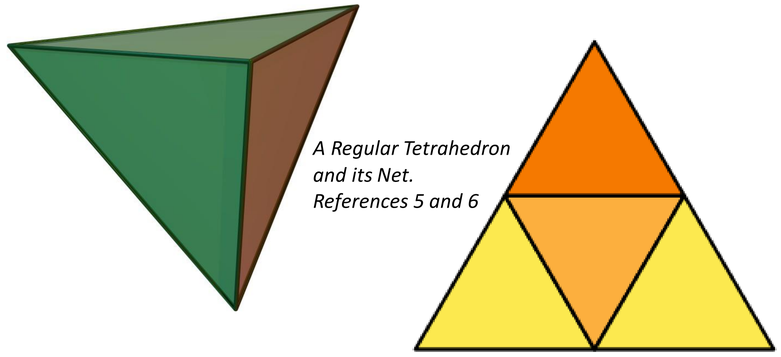
[1] unknown. *The Rotational Symmetries of the Cube*. URL: https://garsia.math.yorku.ca/~zabrocki/math4160w03/cubesyms/. (accessed: 15.12.2020).

[2] unknown. *Theorem (The rotation Group of the Cube). The group of rotations of a cube is isomorphic to S4.* URL: http://facstaff.cbu.edu/~wschrein/media/M402%20Notes/M402L104.pdf. (accessed: 15.12.2020).

The Group Of Symmetries Of The Tetrahedron

Introduction

This poster has been made by Brendan O'Donoghue, Cian Griffin, Paulina Karwan and Stephen Malone for our Groups module MA3343. We are all Mathematics and Education students, and we wanted to use this poster to educate everyone on the symmetries of a Regular Tetrahedron.



A Regular Tetrahedron and its Net. References 5 and 6

Properties and Facts of a Regular Tetrahedron

A Regular Tetrahedron (Also known as a Triangular Pyramid) is a pyramid which has four faces which are all equilateral triangles. Any of the four faces can be considered the base, this will be shown when we describe the symmetries of a Regular Tetrahedron.

A Regular Tetrahedron is a convex polyhedron which can be geometrically described as a polyhedron where any line connecting any two points on the surface of the shape all are contained within the interior of the polyhedron.

It is also one of the five regular Platonic solids which are derived from Eulers formula F(Faces) + V(Vertices) - E(Edges) = 2

A Regular Tetrahedron has Four Triangular Faces, Four Vertex Corners and Six Edges.

Tetrahedrons are represented in real life through chemistry with the structure of molecules (e.g., Methane) and in a four-sided dice which is used less commonly then the six-sided dice.

The group of symmetries of the tetrahedron has 24 elements and it is isomorphic to the symmetric group of degree 4 (the group of all permutations of four objects).

Regular tetrahedron
Solve for volume

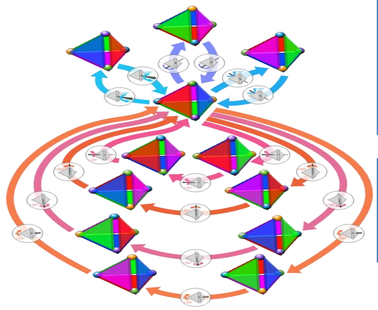
$$V = \frac{a^3}{6\sqrt{2}}$$

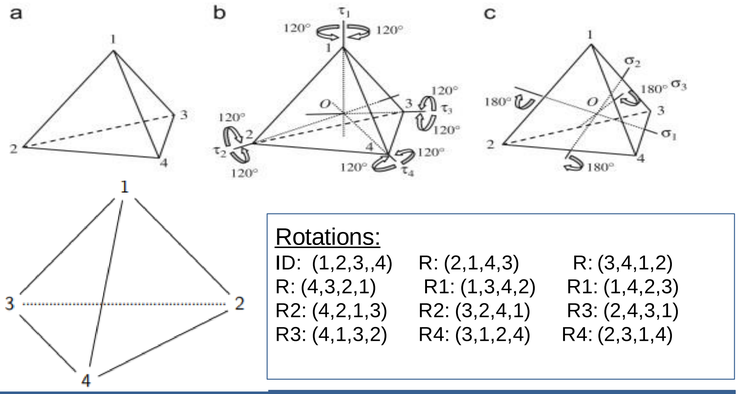
Regular tetrahedron
Solve for surface area

$$A = \sqrt{3}\,a^2$$

Rotations of a tetrahedron

A tetrahedron has 6 axes of symmetry, and it has 12 rotations. In the image below (Fig. X) we see a tetrahedron with vertices labelled 1,2,3 and 4. We will denote a symmetry in this set as a list (i1,i2,i3,i4) where ij is an element of {1,2,3,4} and where ij is the vertex that j is sent to via a symmetry.if we take an example of a rotation- say R1 is the rotation that fixes vertex 1 and rotates the remining vertices on the plane by 2π/3 counterclockwisse, we would write this rotation as (1,3,4,2) with a fixed vertex at 1. As written before, there are 12 rotations . A list of all 12 is given below: (Rotations are labelled R1 meaning rotation with fixed vertex 1")





Rotations:

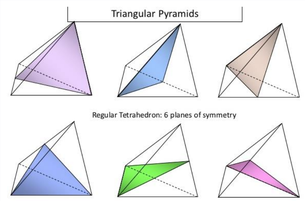
ID: (1,2,3,,4)	R: (2,1,4,3)	R: (3,4,1,2)
R: (4,3,2,1)	R1: (1,3,4,2)	R1: (1,4,2,3)
R2: (4,2,1,3)	R2: (3,2,4,1)	R3: (2,4,3,1)
R3: (4,1,3,2)	R4: (3,1,2,4)	R4: (2,3,1,4)

Reflections of a Tetrahedron

As you can see in the diagram (top right), there are 6 possible planes that can bisect a tetrahedron. Each plane represents a reflection, hence there are 6 different ways to conduct a reflection of a tetrahedron.

In the process of a reflection, the two vertices lying on the plane will become fixed points while the other two vertices will swap positions If we compose a reflection by itself, we will always get the identity element (1,2,3,4).

Another way of justifying that there are 6 reflections of a tetrahedron is, if there are 4 vertices and 2 of them must be chosen and swapped then 4 combinations of 2 will give you 6. i.e. 4C2 = 6.



Reflections

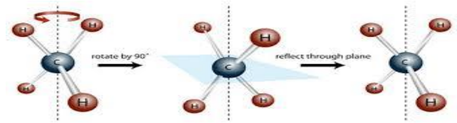
F1:(2,1,3,4)	F4:(1,3,2,4)
F2:(3,2,1,4)	F5:(1,4,3,2)
F3:(4,2,3,1)	F6:(1,2,4,3)

Rotoreflections of a tetrahedron

As we have seen so far, we have 12 rotations and 6 reflections. However, there must be 4!=24 symmetries and we have only discovered 18 of them. The remaining 6 symmetries are called rotoreflections. Rotoreflections are a composition of rotations and reflections. An example of this is in the diagram below of a rotoreflection of the organic tetrahedral compund CH_4 or otherwise known as methane. This compound goes through a rotation of 90° along with a reflection through a plane.

Rotoreflections

RF1:(3,1,4,2)	RF4:(4,3,1,2)
RF2:(3,2,1,4)	RF5:(4,3,2,1)
RF3:(2,3,4,1)	RF6:(3,4,2,1)



The subgroup S4

S4 is a symmetric group with a degree of four. It can be defined as the group of all the permutations of a symmetric group of a set size 4 {1,2,3,4}. Example of this is the symmetries of the tetrahedron.

There are 5 conjugacy classes for the symmetric group s4, they are (1+1+1+1), (2+1+1), (2+2), (3+1), (4). Each of the numbers shown here cycles, e.g. (1+1+1+1) has four cycles of size 1 and (3+1) for example is one cycle of size three with another cycle of size 1.

The group s4 contains all the symmetries of the group of the permutations of the four faces of the regular tetrahedron. As shown in the rotations, reflections and rotorelections we can see the symmetries labelled as shown in permutations to label the symmetries.

Conclusions

To conclude, This is a poster of symmetries, there are 24 symmetries of a tetrahedron, on a regular tetrahedron we can see 4 vertices, 6 edges. It is a geometrical representation of the symmetric group S4.

Our study of group theory has helped us to understand the symmetries of a regular tetrahedron, and hopefully this poster has represented the symmetries well.

References

1. Math.berkeley.edu.[online] Available at: <https://math.berkeley.edu/~mcivor/math113su16/HW/tetrahedron.pdf>
2. Psbbschools.ac.in. 2020. [online] Available at: <http://psbbschools.ac.in/doc/e-magazine-2012/e-mag-tetrahedron.pdf> [Accessed 7 December 2020].
3. Mathworld.wolfram.com. 2020. *Convex Polyhedron -- From Wolfram Mathworld*. [online] Available at: <https://mathworld.wolfram.com/ConvexPolyhedron.html> [Accessed 7 December 2020].
4. En.wikipedia.org. 2020. *Tetrahedral Symmetry*. [online] Available at: <https://en.wikipedia.org/wiki/Tetrahedral_symmetry> [Accessed 7 December 2020].
5. En.wikipedia.org. 2020. *Tetrahedron*. [online] Available at: <https://en.wikipedia.org/wiki/Tetrahedron> [Accessed 7 December 2020].
6. By The original uploader was Cyp at English Wikipedia. - en:User:Cyp/Poly.pov, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=38709

Contact us:

Cian Griffin (18410086)
Stephen Malone (18717531)
Brendan Donoghue (18335816)
Paulina Karwan (18352813)

Examples of Companies with tetrahedral logos

Tetrahedron
Health Nutrition and Cosmetics

Group Theory in Cryptography

Maeve Dunne, Catherine Fraser and Ariea McDaid

Introduction

In the last few years, many papers have proposed cryptosystems based on group theoretic concepts. The idea of group-based cryptosystems is interesting and the different perspective leads to some worthwhile group theory. This poster aims to introduce the use of group theory in public key and symmetric key cryptography systems, with emphasis on **Braid Group Theory** and the **Diffie-Hellman Key Exchange**.

Basics of Cryptography

- Plain text: the original message
- Cipher text: the coded message
- Encryption: the process used for converting the plain text into the cipher text
- Decryption: restoring the plain text from the cipher text

The main technique used in cryptography is based on encryption and decryption. The methods of encryption/decryption fall into two categories: public key and symmetric key. In symmetric key algorithms, the encryption and decryption keys are known to both A and B. In public key cryptography, the encryption key is made public, but it is computationally infeasible to find the decryption key without information known only to B.

Braid Groups

In the last two decades a number of public key cryptosystems based on combinatorial group theoretic problems in braid groups have been proposed. Based on braid groups and its underlying problems, two cryptosystems were suggested by Anshel, Anshel and Goldfeld in 1999 and by Ko, Lee, Cheon, Han, Kong and Park in 2000. These cryptosystems initiated a wide discussion about the possibilities of cryptography in the braid group.

Those underlying problems were as follows:

. Conjugacy decision problem
. Conjugacy search problem
. Multiple simultaneous conjugacy search problem
. Decomposition problem

Some notable key exchange protocols come to mind when on the topic of braid groups:

1. The **Anshel-Anshel-Goldfeld** key exchange protocol which assumes that the conjugacy search problem is difficult. They used the images of braids under the coloured Burau representation of the braid group defined by Marton, instead of the braids themselves.
2. The **Diffie-Hellman** key exchange protocol which is based on the braid group and some commutative property of some of its elements. We will talk more about Diffie-Hellman later.

Although braid groups are not commutative, we can find large subgroups such that each element of the first subgroup commutes with each element of the second and indeed it is true that braids involving disjoint sets of strands commute.

Braid Groups

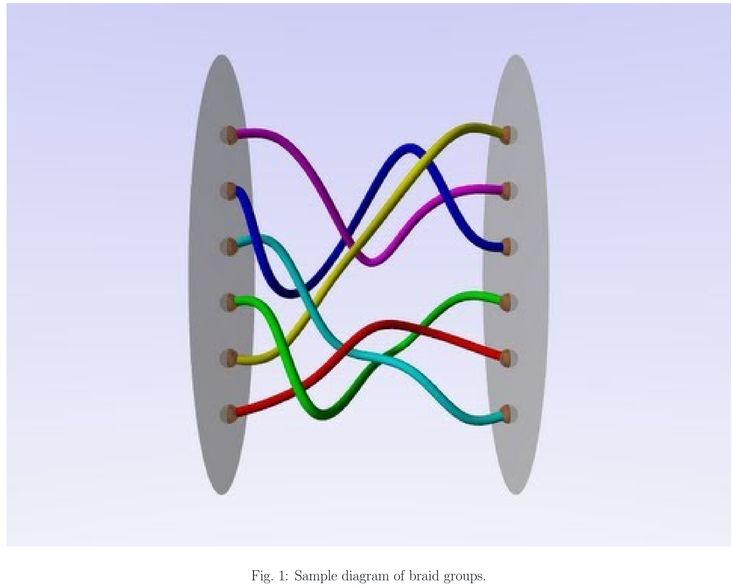


Fig. 1: Sample diagram of braid groups.

Anshel–Anshel–Goldfeld Key Exchange Protocol

Let G be a non-abelian group, and let elements $a_1, ..., a_k, b_1, ..., b_m \in G$ be public.

- Alice picks a private word x in $a_1, ..., a_k$ and sends $b_1^x, ..., b_m^x$ to Bob.
- Bob picks a private word y in $b_1, ..., b_m$ and sends $a_1^y, ..., a_k^y$ to Alice.
- Alice computes x^y and Bob computes y^x.
- The secret key is $[x, y] = x^{-1}y^{-1}xy$.

Note that Alice and Bob can both compute the secret commutator: Alice can premultiply x^y by x^{-1} and Bob can premultiply y^x by y^{-1} and then compute the inverse: $[x, y] = (y^{-1}y^x)^{-1}$.

References

1. "Use of Group Theory in Cryptography" Priya Arora; Assistant Professor, Department of Mathematics, S.D. (P.G) College,Panipat. Vol-2 Issue-6 2016
2. "Group Theory in Cryptography" Simon R. Blackburn, Carlos Cid and Ciaran Mullan. Department of Mathematics, Royal Holloway, University of London. January 25, 2010
3. "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups" Ayan Mahalanobis, Florida Atlantic University. August 2005
4. "New Directions in Cryptography" Whitfield Diffie and Martin E. Hellman, IEEE Transactions on Information Theory Vol. IT-22, No. 6, November 1976

Diffie-Hellman Key Exchange Protocol

"We stand today on the brink of a revolution in cryptography". This was the opening line of a paper published in 1979 by Whitfield Diffie and Martin Hellman, in which they proposed the first publicly known example of a public key cryptosystem; a system now known as the Diffie-Hellman key exchange. It stems from the Discrete Logarithm Problem, namely the complex problem of finding n when given g^n and g. The Diffie-Hellman key exchange can be explained nicely in terms of finite cyclic groups.
We take there to be two parties with no prior knowledge of each other, Alice and Bob, who wish to establish a shared secret key. The steps are as follows below, and a simple example has been included in blue.

1. Alice and Bob agree on a finite cyclic group G with a generating element g, and order n. For our example, let's take $G = (\mathbb{Z}/23\mathbb{Z})^X$, the multiplicative group of integers modulo 23, and the generating element $g = 5$ of this group.
2. Alice chooses a value for a, where a is a natural number and $a < n$, and computes g^a. She sends this value to Bob. Let's say she chooses $a = 4$, then g^a is $5^4 \bmod 23 = 4$. (It is a coincidence that in this case $g^a = a$).
3. Similarly, Bob chooses a natural number b, $b < n$, and computes g^b. He sends this value on to Alice. Bob chooses $b = 3$, so g^b is $5^3 \bmod 23 = 10$.
4. Alice computes $(g^b)^a$, Bob computes $(g^a)^b$, and now both parties are in possession of the shared private key g^{ab}. In our example, Alice computes $(10)^4 \bmod 23 = 18$ and Bob computes $(4)^3 \bmod 23 = 18$. The key is 18.

The choice of group G and generating element g, and the values of g^a and g^b are public knowledge, hence why the Diffie-Hellman key exchange is known as a public key exchange. However the numbers a and b are private and so, thanks to the Discrete Logarithm Problem, it is very difficult for an attacker to obtain the private key g^{ab}.

Logarithmic signatures

There is an *alternative* approach to generalising the Diffie–Hellman scheme: to find a more direct generalisation of the Discrete Logarithm Problem for groups that are not necessarily abelian.

Let G be a finite group, $S \subseteq G$ a subset of G and s a positive integer. For all $1 \leq i \leq s$, let $A_i = [\alpha_{i1}, ..., \alpha_{ir_i}]$ be a finite sequence of elements of G of length $r_i > 1$ and let $\alpha = [A_i, ..., A_s]$ be the ordered sequence of A_i.

We say that α is a *cover* for S if any $h \in S$ can be written as a product $h = h_1...h_s$, where $h_i = \alpha_{ik_i} \in A_i$. If such a decomposition is unique for every $g \in S$, then α is said to be a *logarithmic signature* for S.

One natural way to construct a logarithmic signature for a group G is to take a subgroup chain $1 = G_0 < G_1 < ... < G_n = G$, and let A_i be a complete set of coset representatives for G_{i-1} in G_i. Then $\alpha = [A_i, ..., A_n]$ is a logarithmic signature for G.

THE HISTORY OF LAGRANGE

Emer Forde, Fionnuala Forkan, Eoghan Gallagher

National University of Ireland - Galway

Introduction

Joseph Louis Lagrange was a mathematician in the 18th century, He discovered and proved Lagrange's Theorem. This theorem is seen in the foundations of Group Theory.

This poster will give you an insight to Lagrange's life, the development and proof of his Theorem and uses of his thoerem within Group Theory.

How did Lagrange Discover His Theorem

Linear, Quadratic, Cubic and Quartic equations can be solved using an algebraic formula. Lagrange wanted to find a solution to find the roots of Quintic or higher degree equations. He investigated previous solutions to cubic and quartic equations. He took a different approach to these equations by considering them in terms of permutations of roots.
This was the beginning of group theory before the idea of group theory existed.

He found that cubic and quartic equations can yield an auxillary equation of lower degree (known as a resolvent) which can be used to find the roots of the original polynomial. 'The quartic was solved using a cubic resolvent polynomial whose roots could be written as

$\frac{x_1x_2+x_3x_4}{2}, \frac{x_1x_3+x_2x_4}{2}, \frac{x_1x_4+x_2x_3}{2}$ where x_1, x_2, x_3, x_4

Were the roots of the original polynomial.'[1] These roots can be permuted in every way 4! = 24 and give 3 values. He tried to do this with the quintic equation, which has 5 variables which gives 5! = 120 permutations. He wanted to find an equation that would give either 3 or 4 values within all 120 permutations.

Lagrange did not succeed in this could not find a general formula to solve the quintic and it was later proven to be impossible in the Abel–Ruffini Theorem. However Lagrange did discover his Thoerem during his attempt.

Lagranges Original Thoerem

Lagrange's Original Theorem is not what we see in Group Theory today. In his article Réflexions sur la résolution algébrique des équations, Lagrange states:
'*If a function* $f(x_1, ..., x_n)$ *of* n *variables is acted on by all* $n!$ *possible permutations of the variables and these permuted functions take on only* r *distinct values, then* r *is a divisor of* $n!$.'[1]
This theorem has evolved into a Theorem that can be used in what we call Group Theory


LEÇONS
SUR LA
RÉSOLUTION ALGÉBRIQUE
DES ÉQUATIONS
PAR
M. TORT
Avec une Préface
DE
M. JULES TANNERY
PARIS
LIBRAIRIE NONY & Cie

Fig. 1: Réflexions sur la résolution algébrique des équations

Who was Lagrange

• Joseph Louis Lagrange was born on 25th January 1736 and died in Paris on 10th April 1813. He was an Italian Mathematician and Astronomer. He made significant contributions to the fields of analysis, number theory and mechanics.
• He was educated at the College of Turin where he found a keen interest for mathematics at the age of 17, after reading a memoir by Edmond Halley on the use of algebra in optics.
• At 19 years of age he wrote a letter to Euler in which he solved the isoperimetric problem. The paper draws an analogy between the binomial theorem and the successive derivatives of the product of functions.
• Euler recognized the generality of this methods and its superiority to his own method. This placed Lagrange in the front rank of mathematics of that time.
• On 18 May 1787 he left Berlin after 20 years, to become a member of the Académie des Sciences in Paris, where he remained for the rest of his career.
• Famous Lagrange Quote: "As long as algebra and geometry proceeded along separate paths, their advance was slow and their applications limited. But when these sciences joined company, they drew from each other fresh vitality and thenceforward marched on at a rapid pace toward perfection."

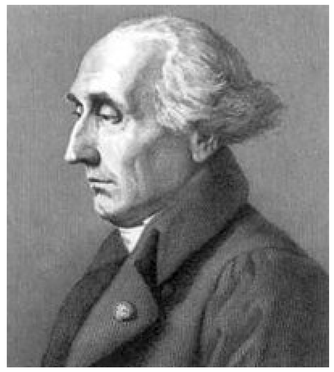


Fig. 2: Lagrange

Lagranges Thoerem

For a finite group G, the order of any subgroup H divides the order of G
Therefore, the order of H is a factor of the order of G.
(order = no. of elements).

Proof

Relies on three lemmas:
• If G is a group with subgroup H then there is a one-to-one correspondence between H and any coset of H
• If G is a group with subgroup H then the left coset relation $g_1 \sim g_2$ if and only if $g_1 * h = g_2 * H$ is an equivalence relation.
• Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq 0$ then $A = B$

Let $\sim$ be the left coset equivalence relation defined in Lemma 2. It follows from Lemma 2 that $\sim$ is an equivalence relation and by Lemma 3 that any two distinct cosets of $\sim$ are disjoint.
Hence, $G = (g_1 * H) \cup (g_2 * H) \cup \ldots \cup (g_l * H)$
Where $g_i * H, \quad i = 1, 2, \ldots, l$ guaranteed by lemma 3.
By lemma 1, the cardinality of each of these cosets is the same as the order of H and so
$|G| = |g_1 * H| + |g_2 * H| + \ldots + |g * H| = |H| + |H| + \ldots + |H|$
L summands $= l * H = l * k$

Lagranges Theorem in C6

Lagranges Theorem can be seen in action for the group of 6 the roots of unity which has all proper subgroups of order 2 or 3 a factor of 6.

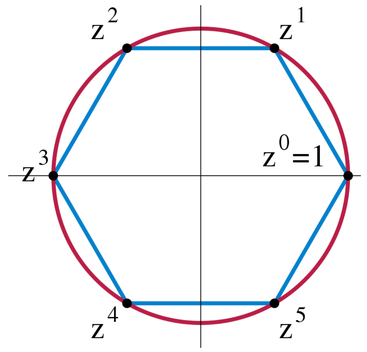


Fig. 3: Cyclic group c6.

Interesting facts about Lagrange

• Lagrange's parents were Italian, although he also had French ancestors on his father's side. In 1787, at age 51, he moved from Berlin to France and became a member of the French Academy, and he remained in France until the end of his life. Therefore, Lagrange is alternatively considered a French and an Italian scientist.
• In 1766 Lagrange succeeded Euler as the director of mathematics at the Prussian Academy of Sciences in Berlin.
• Lagrange's treatise on analytical mechanics, first published in 1788, was the best treatment of classical mechanics since Newton, and helped the development of mathematical physics in the nineteenth century.

Euler - Lagrange Theorem

In the calculus of variations, the Euler-Lagrange equation is a second-order partial differential equation whose solutions are the functions for which a given functional is stationary. This was one of Lagranges large contributions to Mechanics

$$I(x) = \int_b^a F(x(t), x0(t), t)dt$$

References

[1] Richard L. Roth. "A History of Lagrange's Theorem on Groups". In: *Mathematics Magazine* 74.2 (2001), pp. 99–108. ISSN: 0025570X, 19300980. URL: http://www.jstor.org/stable/2690624.

Cyclic Groups and their Generators

Dean Gavagan

† Department of Mathematics, National University of Ireland Galway.

Cyclic Groups and their Properties

A *cyclic group* is a group, all of whose elements are *generated*, by particular element: $x \in G$. We can expand on this and say that G is no more than the set containing all those elements which can be generated from x. When we say x is a *generator*, we mean, simply, that it is a primitive or base element of the set.
For a *cyclic group*, G, we then write: $G =< x >$ and say: x *generates* G.

Properties of Cyclic Groups

- Every cyclic group is abelian. Its group operation is commutative, meaning: $xy = yx \; \forall \; x, y \in G$.
- An important fact arises out of this abelian property: each of conjugacy class of G, consists of only one element. This is why the order of a cyclic group is equal to the order of its generator; since a cyclic group of order n, has n, conjugacy classes.
- A subgroup of a cyclic group is a cyclic group, however cyclic subgroups can appear for non-cyclic groups also.
- If G is a finite finite group, then the order of any elent of G divides G.
- Any two cyclic groups of the same order, whether *finite* or *infinite*, are *isomorphic*.

Finite Cyclic Groups and their Structure

Since a group G is called cyclic if:

$$\exists \; x \in G$$

such that $< x >= G$ and that any such x is called a generator of G.

$$\Rightarrow G =< x >$$

is a cyclic group of order $n < \infty$, then

$$G = e, x, ..., x^n 1$$

,all elements $e, x, ..., x^n 1$ are distinct, and so:

$$x^n = e$$

.

Let $G =< x >$ be a finite cyclic group of order n. The following must hold:

- Every subgroup of G is cyclic and is equal to $< x^d >$. Here we have $d \geq 0$ and $d|n$
- If a and b are positive divisors of n and $a \neq b$, then $< x^a > \neq < x^b >$
- If $k \in \mathbb{Z}$, then x^k is a generator of $G \leftrightarrow k$ and n are coprime.
- For any $k \in \mathbb{Z}$ we have $< x^k >=< x^d >$ where $d = \gcd(n, k)$
- For any $k \in \mathbb{Z}$ we have $o(x^k) = \frac{n}{gcd(n,k)}$

Ultimately, a group is both finite and cyclic if it is isomorphic to the group of integers modulo n for some positive integer n.

Infinite Cyclic Groups

There is only one candidate to exemplify an infinite cyclic group; that is $G = (\mathbb{Z}, +)$, in which case $x =< 1 >, < -1 >$ are the generators. For example; if n is a positive integer, $\mathbb{Z}n$ is a cyclic group of order n generated by 1. We say here, that 1, generates: Z_7, since

$$1 + 1 = 2$$
$$1 + 1 + 1 = 3$$
$$1 + 1 + 1 + 1 = 4$$
$$1 + 1 + 1 + 1 + 1 = 5$$
$$1 + 1 + 1 + 1 + 1 + 1 = 6$$
$$1 + 1 + 1 + 1 + 1 + 1 + 1 = 0$$

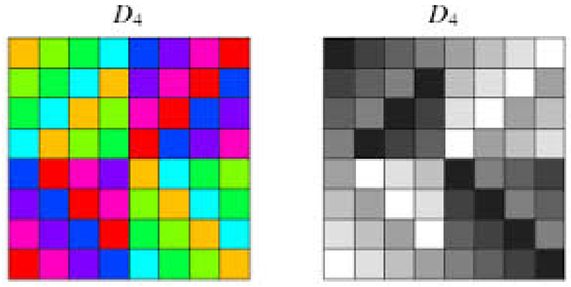
$\mathbb{Z}$ is an infinite cyclic group, because every element is a multiple of ± 1.
More precisely it is the only infinte cyclic group up to isomorphism.

A subsequent lemma of this is that:

$$\forall x \in G, x \neq e \mid \forall m, n \in \mathbb{Z} : m \neq nx m \neq xn$$

Here, e is the identity element of G. That is, such that all the powers of x are distinct.

Examples of Cyclic and Non-cyclic Groups

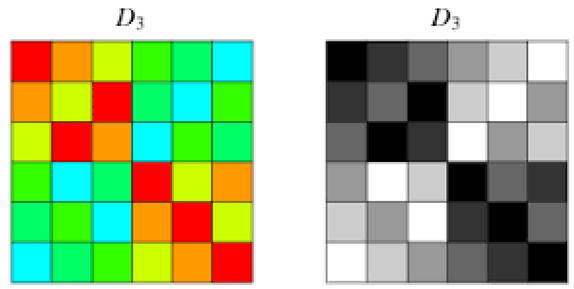


Above are representative group tables, illustrating the inherent pictographic nature of cyclic groups.

In the first figure we have the cyclic dihedral group D_4 dihedral group. In fact, all D_2n dihedral groups are cyclic.

The cycle graph of D_4 as shown, has cycle index given by:

$$\mathbb{Z}(D_4) = \frac{1}{8}x_1^4 + \frac{1}{4}x_2x_1^2 + \frac{3}{8}x_2^2 + \frac{1}{4}x_4.$$



Above are the dihedral groups D_3. It represents an example of a group that is not cyclic in nature and so; no singular element can ever be met with luck in producing all other elements of the group.

The cycle graph of D_3 is shown above. D_3 has cycle index given by:

$$\mathbb{Z}(D_3) = \frac{1}{6}x_1^3 + \frac{1}{2}x_2x_1 + \frac{1}{3}x_3.$$

How Such Groups are Generated

A cyclic group can have more than one generator.
Notice how 3 generates $\mathbb{Z}_{\not 6}$

$$3 + 3 = 6$$
$$3 + 3 + 3 = 2$$
$$3 + 3 + 3 + 3 = 5$$
$$3 + 3 + 3 + 3 + 3 = 1$$
$$3 + 3 + 3 + 3 + 3 + 3 = 4$$
$$3 + 3 + 3 + 3 + 3 + 3 + 3 = 0$$

The group can also be written using multiplicative notation:
Z(7) = {1, a, a2, a3, a4, a5, a6} . In this form, a is a generator of $\mathbb{Z}_{\not 6}$. It turns out that in $\mathbb{Z}(\not 6) = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group. On the other hand, in $\mathbb{Z}(\not 6) = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate.