Unit 10

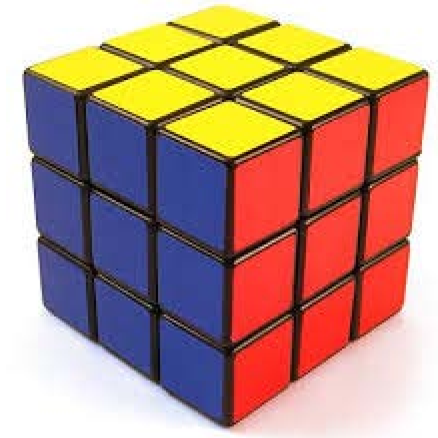
Groups

Why Study Groups?

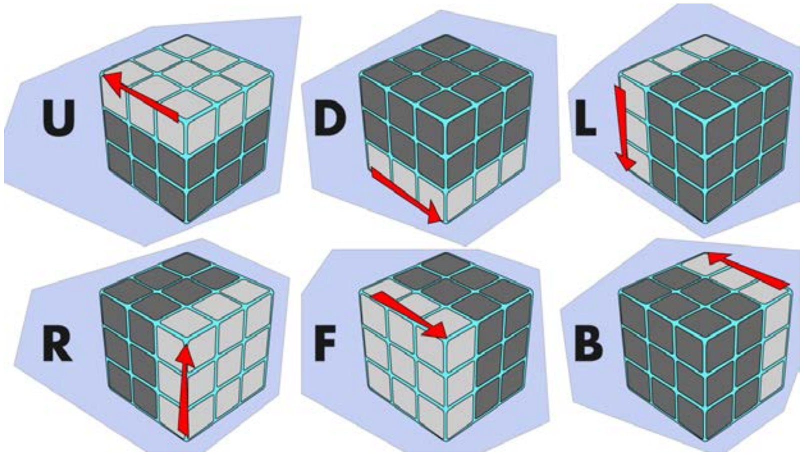
- Group theory is useful for coding & cryptography.
- Application Examples:
  - Coset decoding for linear codes
    - Remark: Coset is a concept of group theory.
  - Group-based cryptography
    - e.g. Diffie-Hellman key exchange uses finite cyclic groups.
- In this unit, only the very basics of group theory will be introduced.
  - We will consider a real-life application to Rubik's cube.

Rubik's Cube

- What will happen if RUR'U' is repeatedly applied?
  - (0.5 min) https://www.youtube.com/watch?v=8zrkSOfzZDk



- How about UL?



Outline of Unit 10

- 10.1 What is Modern Algebra?
- 10.2 Groups
- 10.3 Groups of Symmetry
- 10.4 Rubik's Cube

Unit 10.1

What is Modern Algebra?

The Origin of "Algebra"

- "Algebra" is derived from the Arabic word "al-jabr".
  - First used by the Persian mathematician, Muhammad Al Khwarizmi, in the title of his mathematics book.
  - It roughly means "reunion", which describes the method for collecting terms of an equation in order to solve it.

Algebra = Solving Equations

Muhammad Al Khwarizmi (780-850), the Father of Algebra.

Classical Age of Algebra

- Methods to solve linear and quadratic equations were known in ancient times.
  - $ax + b = 0$
  - $ax^2 + bx + c = 0$
- Cubic and quartic equations were solved in the 16th century.
  - $x^3 + ax^2 + bx = c$
  - $x^4 + ax^3 + bx^2 + cx = d$

How about *quintic* equation?

Degree	Name
0	Constant
1	Linear
2	Quadratic
3	Cubic
4	Quartic
5	Quintic
6	Sextic or Hexic
7	Septic or Heptic
8	Octic
9	Nonic
10	Decic

Modern Age of Algebra

Niels Henrik Abel (1802-1829), a Norwegian mathematician.

Évariste Galois (1811-1832), a French mathematician.

- In 1824, Abel showed that there does not exist any formula for the roots of an equation whose degree is 5 or above.

- Later, Galois laid the foundation for a branch of mathematics known as group theory.
  - https://www.youtube.com/watch?v=Mc0bvea6G3I (3.5 min)

What is Modern Algebra?

- Modern algebra is also called abstract algebra.

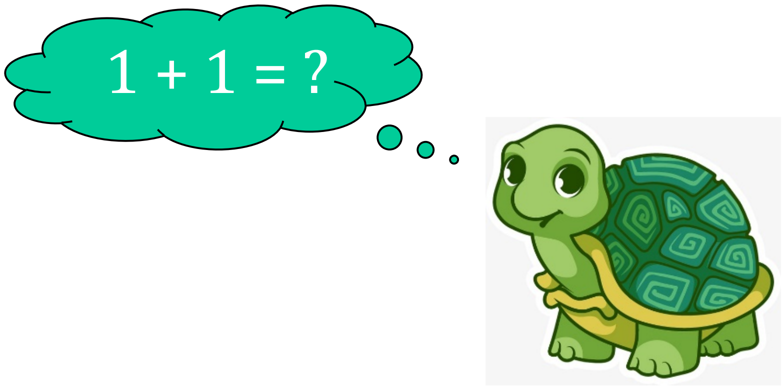
Algebra = Study of Algebraic Structures

- Examples of algebraic structures:
  - groups, rings, fields, vector spaces, modules, etc.
- Watch the 3-min video:
  - https://www.youtube.com/watch?v=IP7nW_hKB7I&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6

Abstract algebra will challenge you like never before.

Algebraic Structures

- An algebra consists of
    i. a set of elements, and
    ii. one or more operations on the set.
- Operation: a way of combining two elements of the set to produce an element of the same set.
- Example: The set of integers with addition.



Identity and Inverse

- Consider a set S and an operation $*$.
- Definition:
  - An element $e \in S$ is called the identity if
    $$x * e = e * x = x \text{ for all } x \in S.$$
  - An element $y \in S$ is called the inverse of x if
    $$x * y = y * x = e.$$
- Example: The set of integers with addition.
  a) Identity?
  b) Inverse of 1?

Example: Boolean Algebra for Sets

Set Union

- Commutative
  - $A \cup B = B \cup A$
- The empty set $\emptyset$ is the identity element for $\cup$
  - $A \cup \emptyset = A$
- No inverse

Set Intersection

- Commutative
  - $A \cap B = B \cap A$
- The universal set U is the identity element for $\cap$.
  - $A \cap U = A$
- No inverse

- Distributive
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- And many others rules…

Example: Matrix Algebra

Addition

- Matrices can be added
  - $A + B$ is also a matrix.
- Commutative
  - $A + B = B + A$.
- Zero matrix
  - $A + 0 = A$.
- Additive inverse exists (so subtraction can be performed).
  - $A + C = 0$ (C always exists)

Multiplication

- Matrices can be multiplied
  - AB is also a matrix.
- Non-commutative
  - $AB \neq BA$ (in general)
- Identity matrix
  - $AI = A$
- Multiplicative inverse may or may not exist.
  - $AC = I$ (C may or may not exists)

Algebraic Structures

Structures	Operations (that satisfy certain properties)	Examples
Group	Addition & Subtraction	24-Hour Clock (16:00 + 1:50 = ?)
Ring	Addition, Subtraction, & Multiplication	Integers, Modulo q (where q is a composite number).
Field	Addition, Subtraction, Multiplication & Division (except 0)	Rational Numbers, Real Numbers, Complex Numbers, Modulo p (where p is prime).
Vector Space	Scalar Multiplication & Division (except 0), Vector Addition & Subtraction	Real vector space, complex vector space, binary vector space.

- We consider only groups in this unit.

Unit 10.2

What is a Group?

The Definition of Groups

- A set of elements, G, with an operation (denoted by $*$)
  - We denote it by $\langle G, * \rangle$.

1. Closure under $*$
   - $x, y \in G \Rightarrow x * y \in G$
2. There exists an identity element $e \in G$
   - $y * e = e * y = y,$ for all $y \in G$
3. Inverse $x^{-1} \in G$ exists for all $x \in G$
   - $x * x^{-1} = x^{-1} * x = e$
4. Associativity of $*$
   - $(a * b) * c = a * (b * c)$

4

Definition of Groups: (3 min):
https://www.youtube.com/watch?v=QudbrUcVPxk&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6&index=2

Abelian Groups

- In the definition of groups, the operation is *not* required to be *commutative*.
  - That is, $x * y$ is not required to be equal to $y * x$.
  - Note: identity and inverse are defined for both sides.
- If the commutative rule applies, then the group is called a commutative group or an Abelian group.

Classwork: The Set of Integers

a) Is $\langle \mathbb{Z}, + \rangle$ a group?

- [ ] Closure
- [ ] Identity
- [ ] Inverse
- [ ] Associativity

b) Is $\langle \mathbb{Z}, \times \rangle$ a group?

- [ ] Closure
- [ ] Identity
- [ ] Inverse
- [ ] Associativity

Example: Addition Modulo n

- For illustration, suppose $n = 4$.
- $G = \{0, 1, 2, 3\}$ with addition mod 4
  - Closed under $+$
    - For any $x, y \in G,\ x + y \pmod 4 \in G$
  - Identity element: 0
    - For any $x \in G,\ 0 + x = x + 0 = x.$
  - Inverse exists.
    - For any $x \in G,\ x^{-1} = 4 - x.$
  - Associativity:
    - $(x + y) + z \pmod 4 = x + (y + z) \pmod 4.$
- We denote the *additive group of integers mod n* by $\mathbb{Z}_n$.
    - (In some books, it was written as $\mathbb{Z}/n\mathbb{Z}$.)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Uniqueness of Identity and Inverse

- There is only one single identity element in G.
  - Suppose e_1 and e_2 are both identity elements.
  - Since e_1 is an identity, $e_1 * e_2 = e_2$.
  - Since e_2 is an identity, $e_1 * e_2 = e_1$.
  - Hence, $e_1 = e_2$.
- For each $x \in G$, there is only one single $x^{-1} \in G$.
  - Suppose y_1 and y_2 are both inverses of x.
  - $y_1 * (x * y_2) = y_1 * e = y_1$
  - $(y_1 * x) * y_2 = e * y_2 = y_2$
  - Since $*$ is associative, $y_1 = y_2$.

Classwork: Binary Vector Space

- Is $\langle \mathbb{B}^n, + \rangle$ a Group, where $+$ denotes bitwise XOR.

  - [ ] Closure
  - [ ] Identity
  - [ ] Inverse
  - [ ] Associativity

Notation

- There are two common ways to denote the operator $*$ and the identity element e:

Addition: $+$
Identity: 0

Multiplication: $\times$
Identity: 1

$a \times b$ is often simplified as ab.

$a^n = a \times a \ldots \times a.$ (n times)
$a^0 = 1$ (or denoted by e)

Order (two different senses)

- The *order* of a *group* G, denoted by $|G|$, is the number of elements in G.
  - Just like the cardinality of a set.

- The *order* of an *element* $x \in G$, denoted by $|x|$ or $\mathrm{ord}(x)$, is the smallest positive integer n such that $x^n = e$.
  - It represents how long it takes *to reach the identity*.
- If there is no such n, then the order of x is infinity.

Classwork

- Consider the set of non-zero real numbers with multiplication.

a) Is it a group? Why is zero excluded?

- [ ] Closure
- [ ] Identity
- [ ] Inverse
- [ ] Associativity

b) What are the orders of the elements of this set?

Cayley Table

- Cayley table is also called group multiplication table.
  - You have seen one in a previous example.
- Just like how you learnt multiplication in the primary school.

The identity e is usually put in the first entry.

$*$	e		y	
e				
x			$x * y$	

Multiplication Table 1 x 10

x	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

Example: $\{1, -1, i, -i\}$ with $\times$

$\times$	$\mathbf{1}$	$\mathbf{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	-1

- The table is *symmetric* across the diagonal.
  - Because this group is Abelian, i.e., $a \times b = b \times a$.
- No *duplicate* elements in every row and column.
  - Why? Watch this (7.5 min):
    - https://www.youtube.com/watch?v=BwHspSCXFNM&index=9&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6

Groups of Orders 1, 2 and 3

*	$\boldsymbol{e}$
$\boldsymbol{e}$	e

Group of order 1, the trivial group.

*	$\boldsymbol{e}$	$\boldsymbol{a}$
$\boldsymbol{e}$	e	a
$\boldsymbol{a}$	a	e

Group of order 2, $\mathbb{Z}_2$.

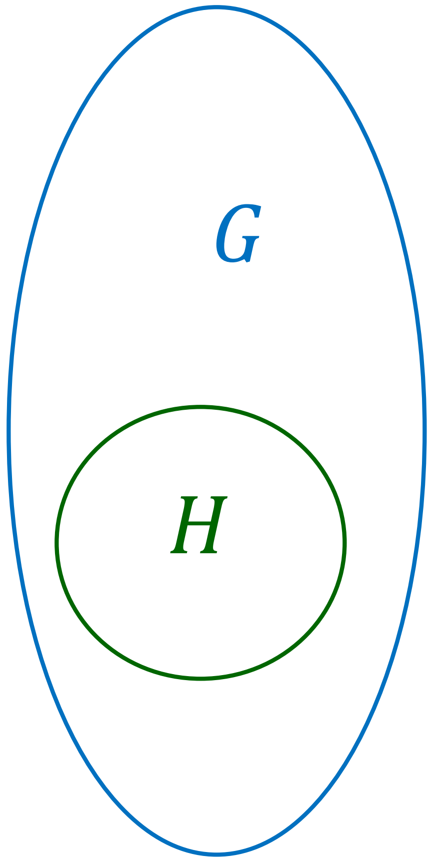
*	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$
$\boldsymbol{e}$	e	a	b
$\boldsymbol{a}$	a	b	e
$\boldsymbol{b}$	b	e	a

Group of order 3, $\mathbb{Z}_3$.

- Filling in Cayley table is kind of like solving Soduku puzzle.
  - Each row and each column must contain all the elements of the group.

Subgroups

- Consider $\langle G, * \rangle$, $H \subseteq G$, and $H \neq \emptyset$.
- If $\langle H, * \rangle$ is a group, then H is a subgroup of G, denoted by $H \leq G$.
- Two standard subgroups:
  - The group itself: $\langle G, * \rangle$
  - Trivial subgroup: $\langle \{e\}, * \rangle$
- Example:
  - The set of integers with addition is a group.
  - The set of even numbers with addition is its subgroup.



Classwork

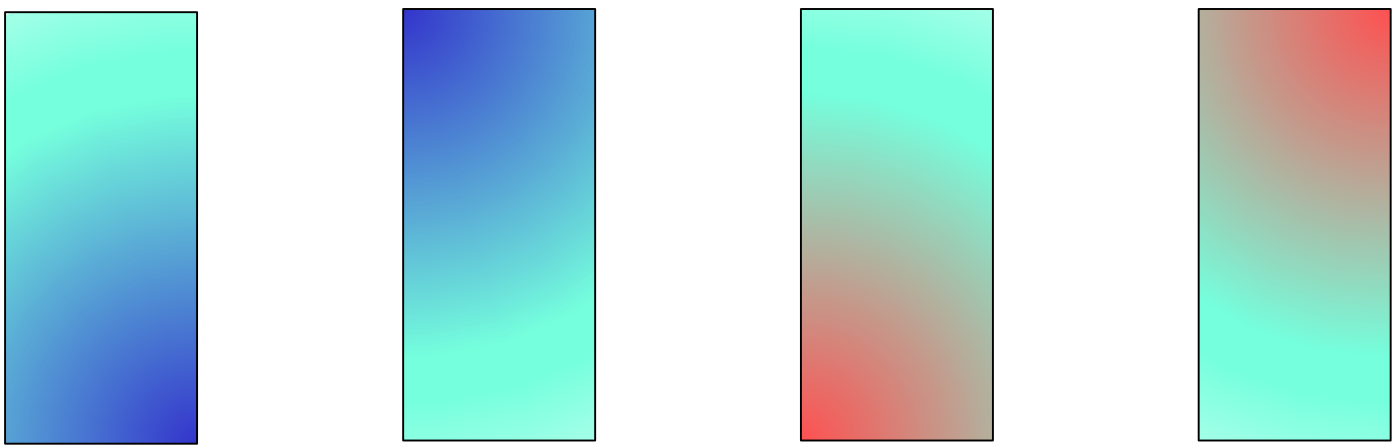
a) $\langle \mathbb{R}, + \rangle$ is a group. Is $\langle \mathbb{Z}, + \rangle$ its subgroup?

b) $\langle \mathbb{R} \backslash \{0\}, \times \rangle$ is a group. Is $\langle \mathbb{Z} \backslash \{0\}, \times \rangle$ its subgroup?

Unit 10.3

Groups of Symmetry

Groups of Symmetry for Rectangles



Is this an Abelian group?

identity e | rotate 180^o r | flip f | flip & then rotate rf

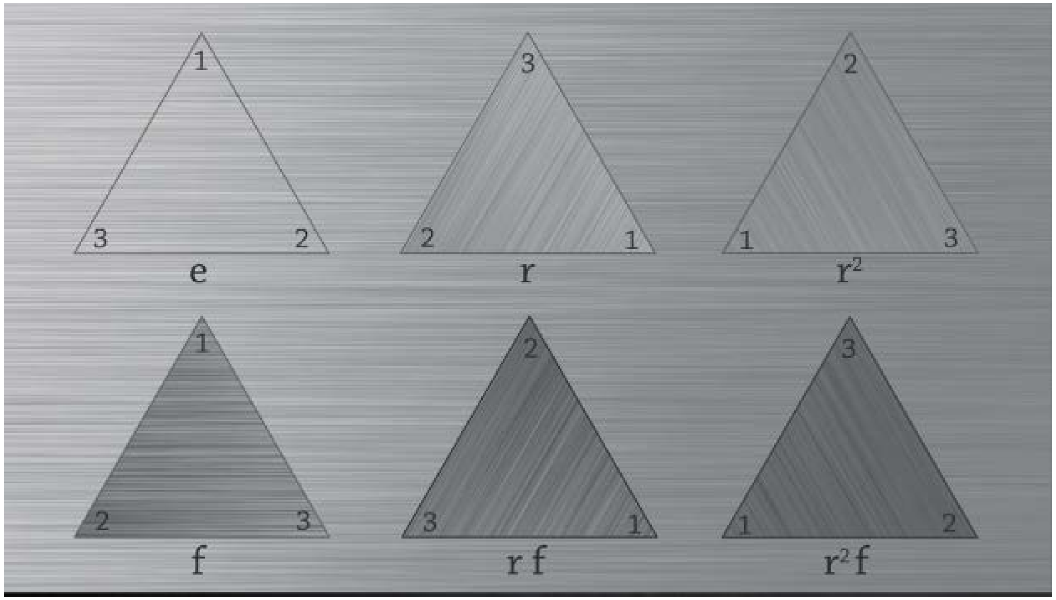
- There are four group elements e, r, f, rf.
  - They are geometric transformations, which are functions.
- The group operation is *function composition* $\circ$.
  - e.g. $r \circ f = rf$

Groups of Symmetry for Rectangles

- Multiplication Table:

$\circ$	e	r	f	rf
e	e	r	f	rf
r	r	e	rf	f
f	f	rf	e	r
rf	rf	f	r	e

Groups of Symmetry for Triangles



Is this an Abelian group?

- There are six group elements $e,\ r,\ r^2,\ f,\ rf,\ r^2f$.
- How about isosceles triangles & scalene triangles?
  - (4 min) https://www.youtube.com/watch?v=DeCcqioogLY

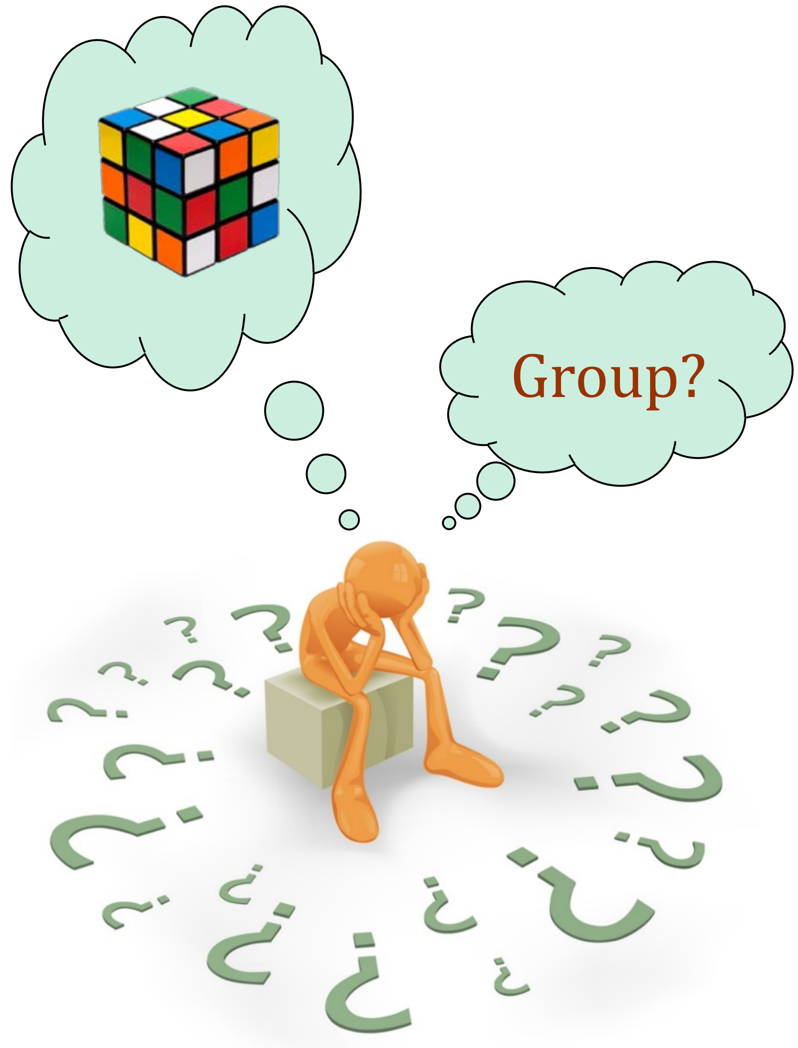
Unit 10.4

Rubik's Cube

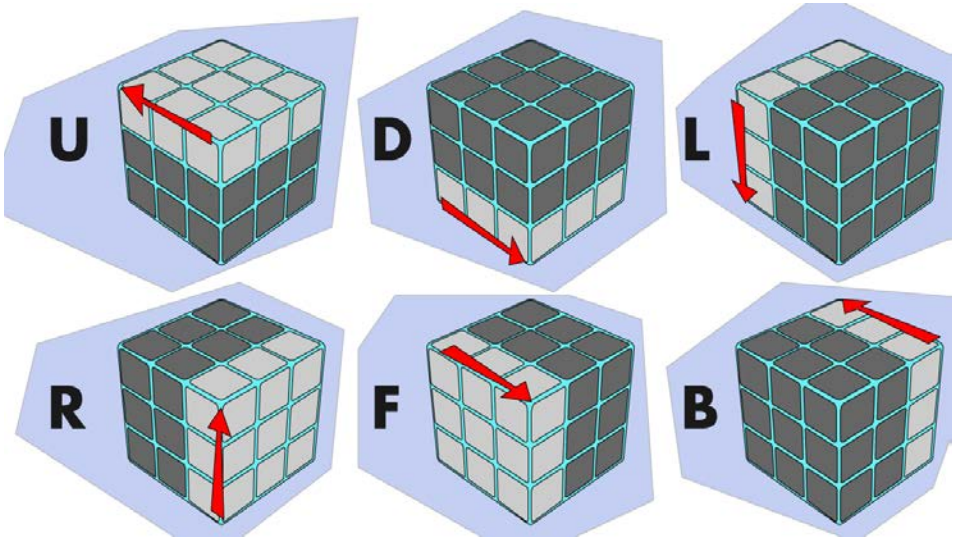
Rubik's Cube

- A 3-D combination puzzle invented in 1974.
- Highly popular in the 1980's.
- Widely considered the world's best-selling toy.

- Can you see that a group can be defined on it?



Notation



- Six basic moves:
  - Right (R), Left (L)
  - Front (F), Back (B)
  - Up (U), Down (D)
- A move is any *sequence* of these six basic moves.
  - e.g. RU, RRR, etc.
- Two moves are considered the same if they result in the same configuration of the cube.
  - e.g., RRRRR is the same as R (why?)

Rubik's Cube as a Group $\langle G, * \rangle$

- G: the set of all possible moves.
  - $|G| = 43{,}252{,}003{,}274{,}489{,}856{,}000 = 2^{27}3^{14}5^{3}7^{2}11$

- $M_1 * M_2$ means the move M_1 followed by M_2.
  - Caution: The concept is just function composition, but the notation is *different*.
  - Examples:
    - RR $*$ UR is the same as RRUR.
    - RR * RRR is the same as RRRRR = R.

Group Properties: Verification

- Closure
  - $M_1 * M_2$ is certainty a move.
- Identity
  - e means doing nothing.
- Inverse
  - Any basic move has an inverse, e.g., R' = RRR.
  - Given any move M, simply reverse the steps in M to obtain its inverse (denoted by M')
  - e.g., (RUF)' = F' U' R'
- Associativity
  - Let C be a configuration of the Rubik's cube.
  - Define $M(C)$ as the resultant configuration after applying M to C.
  - Applying $M_1 * M_2$ to C is the same as $M_2(M_1(C))$.
  - We want to prove

    $$(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$$

  - L.H.S. = $M_3\big((M_1 * M_2)(C)\big)$

    $$= M_3\left(M_2\big(M_1(C)\big)\right)$$

  - R.H.S. = $(M_2 * M_3)\big(M_1(C)\big)$

    $$= M_3\left(M_2\big(M_1(C)\big)\right)$$

Classwork

a) Is $\langle G, * \rangle$ Abelian?

b) Can you identify a subgroup of order 4?

c) Will the original position be reached if UL is repeated indefinitely?

Order

Theorem: Any element of a finite group has a finite order.

Proof:

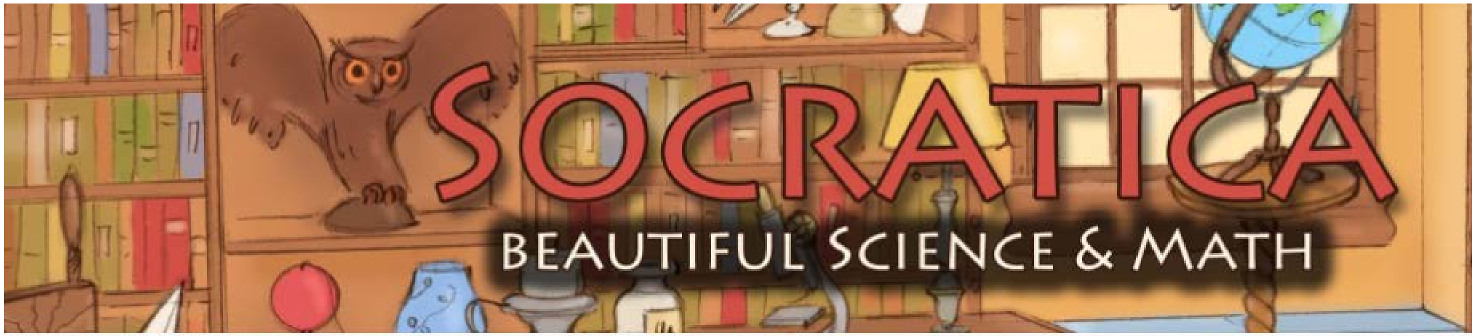
- Pick an arbitrary element a.
- Consider $a, a^2, a^3, a^4, \dots, a^m, \dots, a^n$.
- Since the group is finite, the elements must repeat.
- Let a^n be the first repeated element in the above list and $a^m = a^n$.
- Then $a^{n-m} = e$.
- The order of a is $n - m$, which is finite. *Q.E.D.*

Order of Elements in G

Examples:

- ord$(RUR'U') = ?$ (try it yourself!)
- ord$(UL) = 63$
- ord$(RU^2D'BD') = 1260$ (the largest order)

Abstract Algebra on YouTube

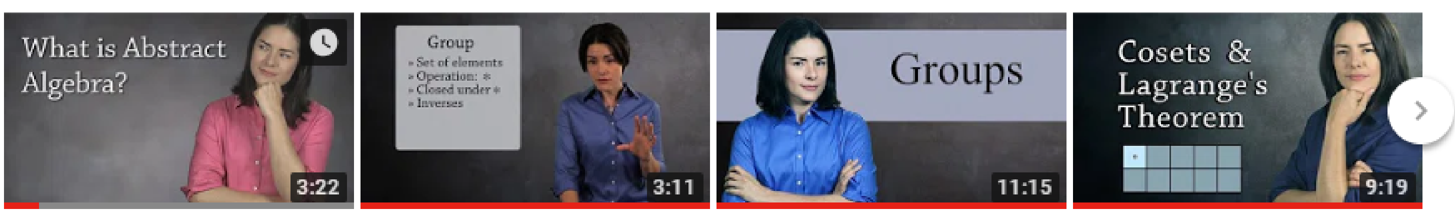


Socratica
訂閱人數：264,241

I *highly recommend* the YouTube video series of Abstract Algebra by Socratica.

Abstract Algebra 全部播放

Abstract Algebra deals with groups, rings, fields, and modules. These are abstract structures which appear in many different branches of mathematics, including geometry, number theory, topology,



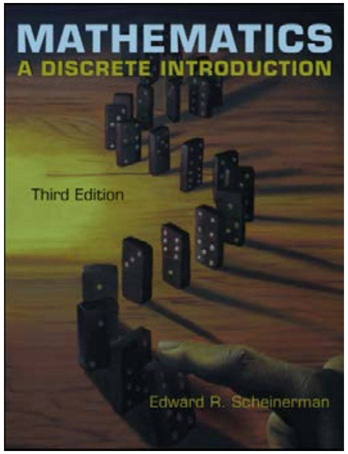
What is Abstract Algebra? (Modern Algebra)
Socratica
觀看次數：19萬 次・2 年前
字幕

Abstract Algebra: The definition of a Group
Socratica
觀看次數：18萬 次・5 年前
字幕

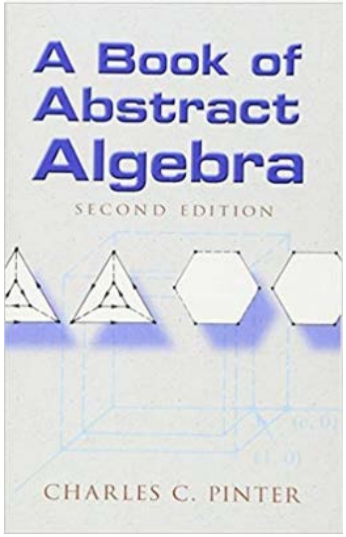
Group Definition (expanded) - Abstract Algebra
Socratica
觀看次數：9.4萬 次・11 個月前
字幕

Cosets and Lagrange's Theorem - The Size of...
Socratica
觀看次數：12萬 次・1 年前

Recommended Reading



- Chapter 8, E. A. Scheinerman, *Mathematics: A Discrete Introduction*, 3rd ed., Cengage Learning, 2012.



- Chapters 3-5 and 7, C. C. Pinter, *A Book of Abstract Algebra*, 2nd ed., Dover Publications, 2010.