Abstract Algebra Part 1

Disclaimer: Work in progress. Portions of these written materials are incomplete.

Group Theory

What is group theory?

- Group theory is the **study of symmetry**

What is group theory?

- Group theory is the **study of symmetry**
- **Symmetries** are structure-preserving transformations

What is group theory?

- Group theory is the **study of symmetry**
- **Symmetries** are structure-preserving transformations
- Group theory is historically important and still widely-studied and researched today

What is group theory?

- Group theory is the **study of symmetry**
- **Symmetries** are structure-preserving transformations
- Group theory is historically important and still widely-studied and researched today
- Group theory underpins more advanced topics in abstract algebra

Why is symmetry important?

- In Physics: Noether's Theorem
    - Continuous symmetries explain why momentum, angular momentum, and energy are conserved quantities

Why is symmetry important?

- In Physics: Noether’s Theorem
  - Continuous symmetries explain why momentum, angular momentum, and energy are conserved quantities
- In Chemistry: group theory helps understand the structure and stability of molecules
  - The symmetries of a molecule can be used to predict some of a molecule’s properties

Why is symmetry important?

- In Physics: Noether's Theorem
  - Continuous symmetries explain why momentum, angular momentum, and energy are conserved quantities
- In Chemistry: group theory helps understand the structure and stability of molecules
  - The symmetries of a molecule can be used to predict some of a molecule's properties
- In Mathematics:
  - Abel-Ruffini Theorem: insolvability of polynomials of degree > 4

Why is symmetry important?

- In Physics: Noether's Theorem
  - Continuous symmetries explain why momentum, angular momentum, and energy are conserved quantities
- In Chemistry: group theory helps understand the structure and stability of molecules
  - The symmetries of a molecule can be used to predict some of a molecule's properties
- In Mathematics:
  - Abel-Ruffini Theorem: insolvability of polynomials of degree > 4
  - We often study complex objects by studying their symmetries, which are typically simpler and yield useful information

[Emmy] Noether's theorem

- Deep result linking algebra and theoretical physics, proven by Emmy Noether (1918)

[Emmy] Noether's theorem

- Deep result linking algebra and theoretical physics, proven by Emmy Noether (1918)
- Every continuous symmetry of a physical system has a corresponding conservation law

[Emmy] Noether's theorem

- Deep result linking algebra and theoretical physics, proven by Emmy Noether (1918)
- Every continuous symmetry of a physical system has a corresponding conservation law
- Applies to classical systems
  - For example, invariance in space $\longleftrightarrow$ conservation of momentum
  - Invariance in time $\longleftrightarrow$ conservation of energy

[Emmy] Noether's theorem

- Deep result linking algebra and theoretical physics, proven by Emmy Noether (1918)
- Every continuous symmetry of a physical system has a corresponding conservation law
- Applies to classical systems
  - For example, invariance in space ⟵⟶ conservation of momentum
  - Invariance in time ⟵⟶ conservation of energy
- Also applies to quantum mechanics
  - Conservation of particle properties such as charge

[Emmy] Noether's theorem

- Deep result linking algebra and theoretical physics, proven by Emmy Noether (1918)
- Every continuous symmetry of a physical system has a corresponding conservation law
- Applies to classical systems
  - For example, invariance in space ⟵⟶ conservation of momentum
  - Invariance in time ⟵⟶ conservation of energy
- Also applies to quantum mechanics
  - Conservation of particle properties such as charge
- Excellent videos on this topic here

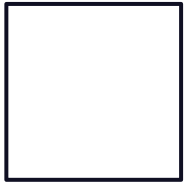
Emmy Noether

- One of the most important mathematicians of the 20th century
  - Often described as the most important woman mathematician
- She also made foundational contributions to abstract algebra
  - In a time when women faced barriers attending universities (1920s)
- Crucial results including the pervasive [isomorphism theorems]
- Many key definitions created by or named after her

Cyclic Groups

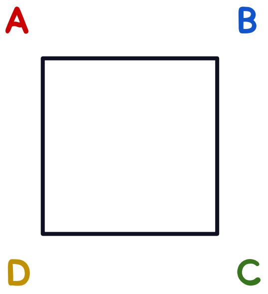
Symmetries of a Square

Rotations of a square



Symmetries of a Square

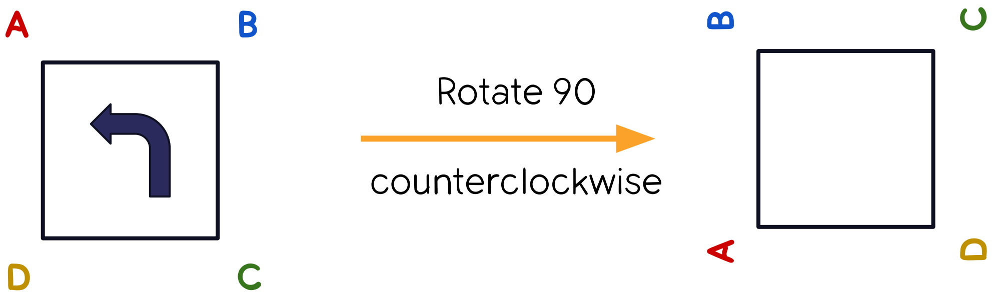
Rotations of a square



Let's label the corners to keep track of the the order and orientation of the square

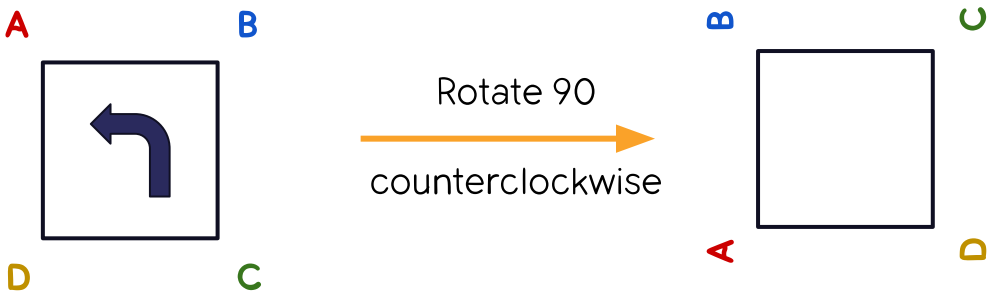
Symmetries of a Square

Rotations of a square



Symmetries of a Square

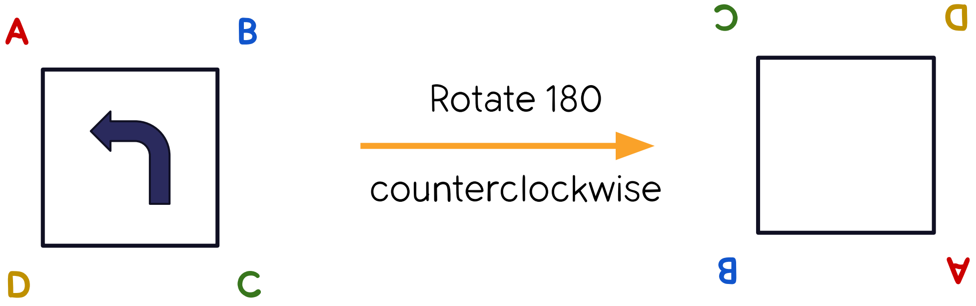
Rotations of a square



Technical term for this kind of symmetry: **plane isometry**

Symmetries of a Square

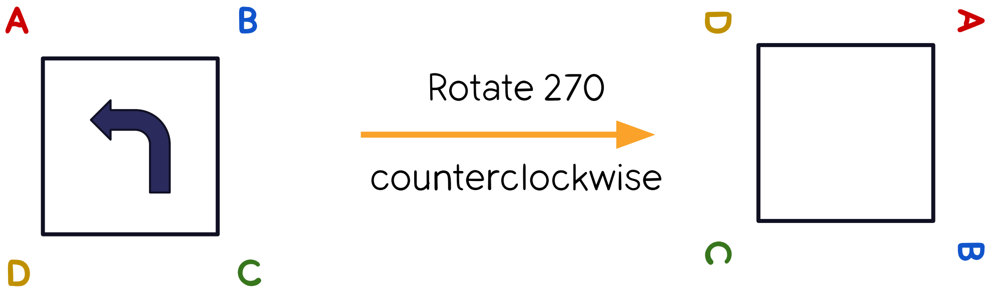
Rotations of a square



Same as 90 degrees twice

Symmetries of a Square

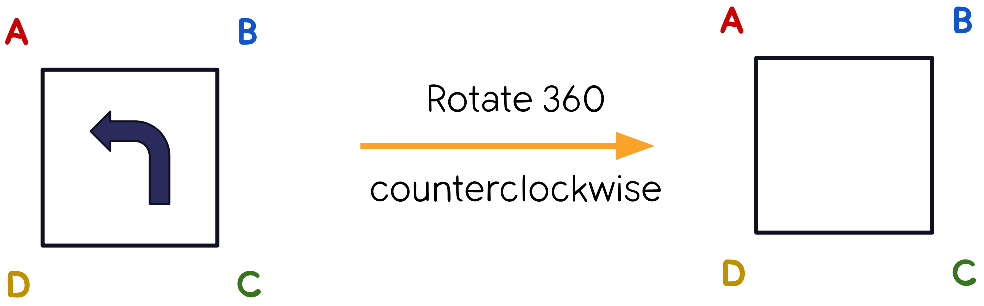
Rotations of a square



Same as 90 degrees thrice

Symmetries of a Square

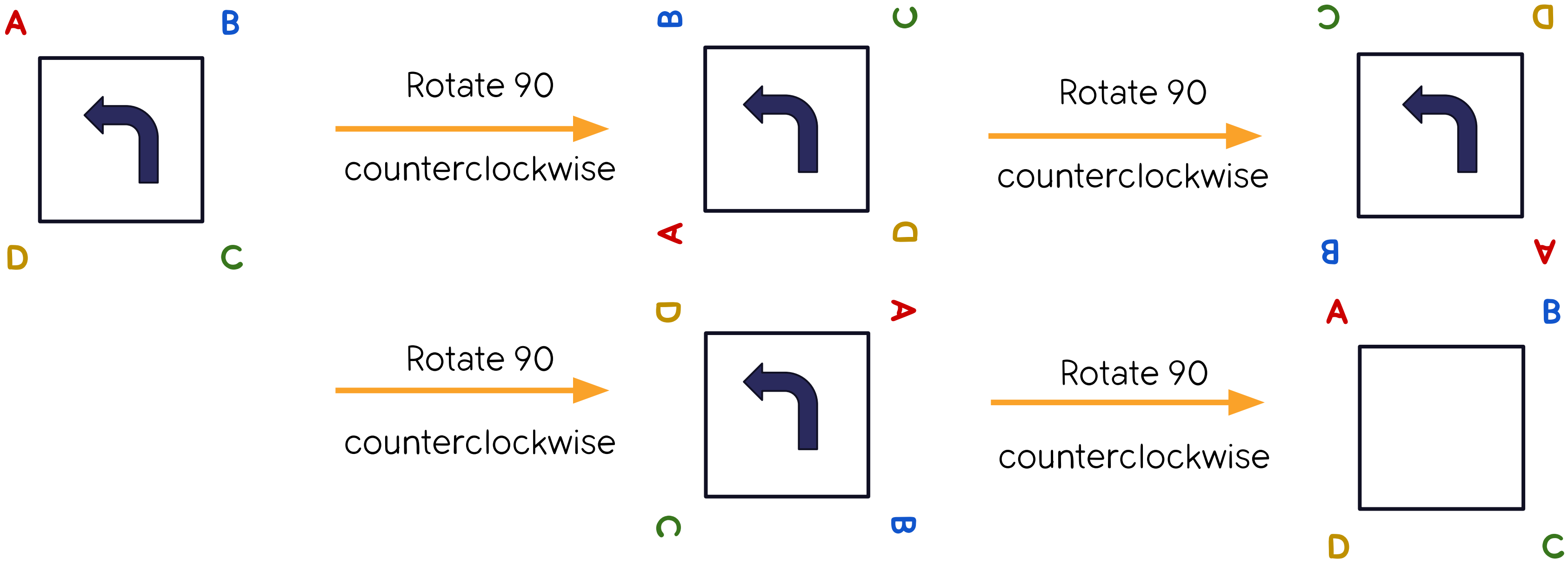
Rotations of a square



Back to the original after four rotations! This is called the **identity** transformation

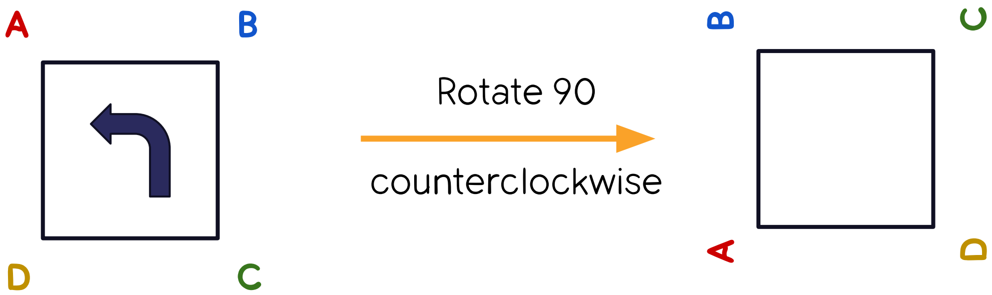
Symmetries of a Square

Applying the 90 rotation four times brings up back to the original



Symmetries of a Square

Algebraically:

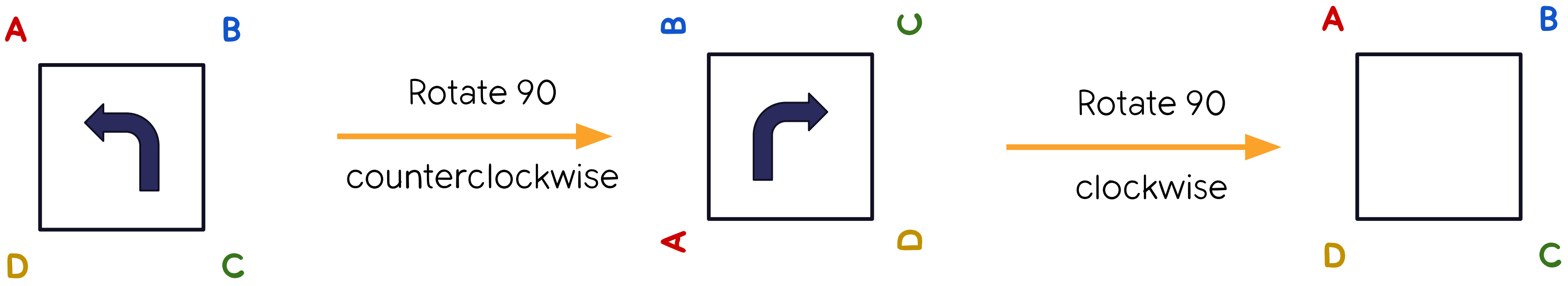


Let's call the rotation **r**. Then rotating four times brings us back to the original we say this symbolically by

$$r^4 = 1$$

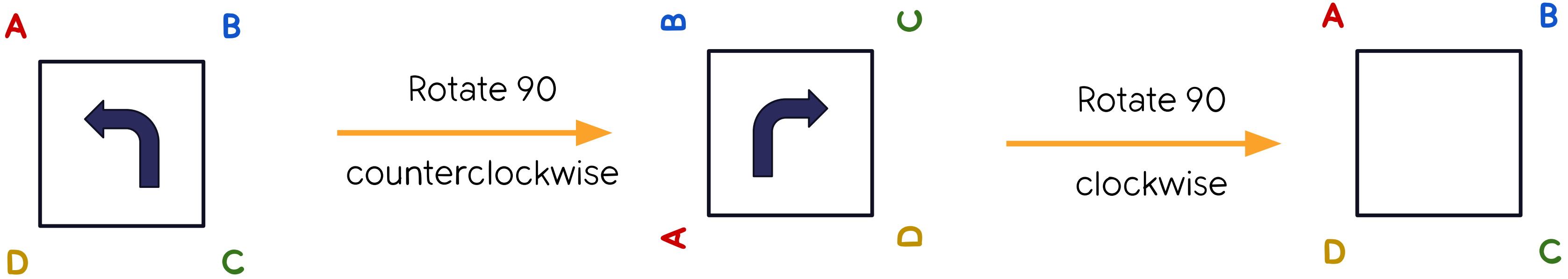
Symmetries: invertible / reversible

- Each structure preserving transformation can be reversed
  - Rotate 90 counterclockwise, rotate clockwise 90 to undo



Symmetries: invertible / reversible

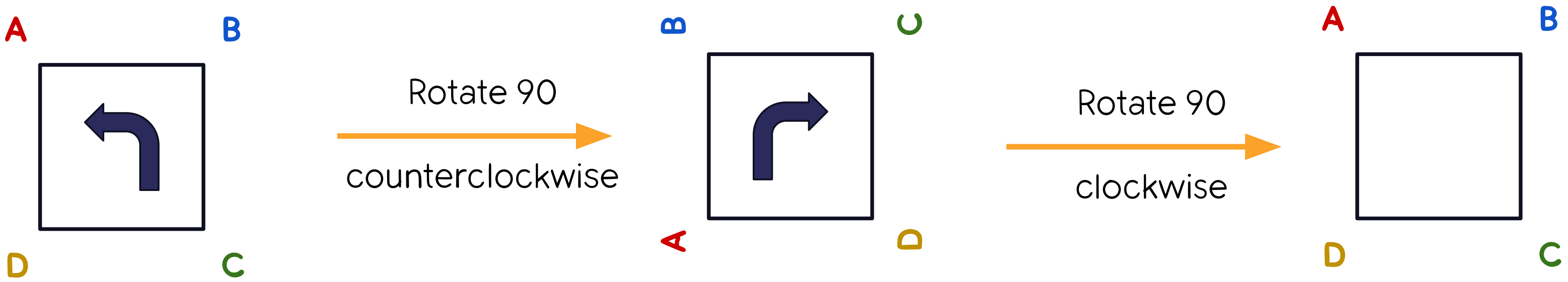
- Each structure preserving transformation can be reversed
  - Rotate 90 counterclockwise, rotate clockwise 90 to undo



Call this transformation r and this one r^{-1}

Symmetries: invertible / reversible

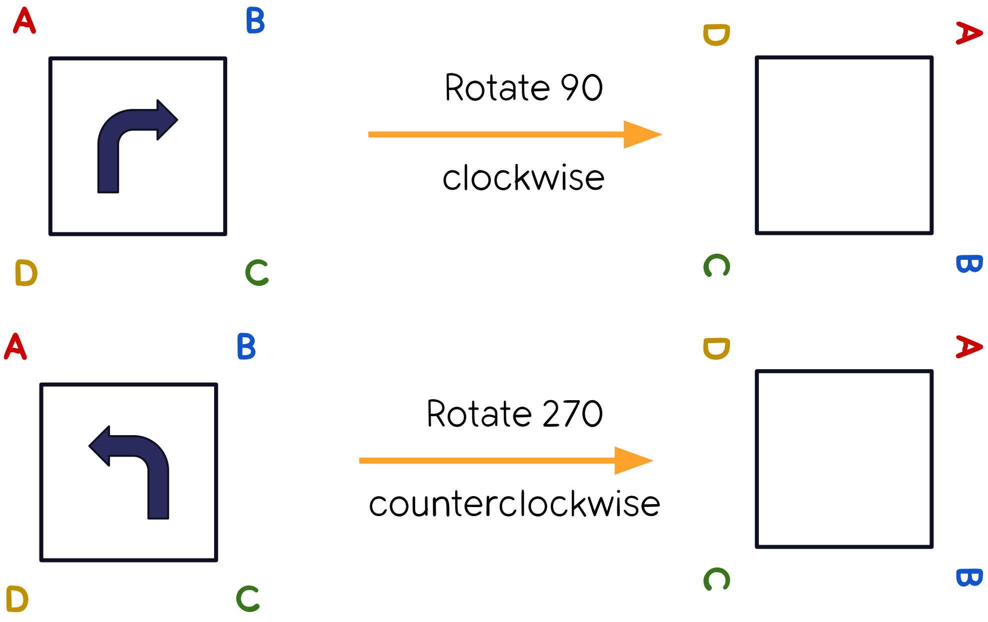
- Each structure preserving transformation can be reversed
    - Rotate 90 counterclockwise, rotate clockwise 90 to undo



Then we have that $r * r^{-1} = r^0 = 1 = r^{-1} * r$

Symmetries: invertible / reversible

- Each structure preserving transformation can be reversed
    - Rotate 90 counterclockwise, rotate clockwise 90 to undo



Also, a clockwise rotation of 90 is the same as a counterclockwise rotation of 270

$$r^{-1} = r^3$$

$$r^4 = 1$$

Symmetries of a Square: rotations

- So, the rotations of a square give us four transformations
- The identity 1, which is a rotation of 0 degrees (or any multiple of 360)
- The three rotations 90, 180, and 270 degrees
    - The inverse rotations are included here, since -90 == 270, -180 == 180

Symmetries of a Square: rotations

- So, the rotations of a square give us four transformations
- The identity 1, which is a rotation of 0 degrees (or any multiple of 360)
- The three rotations 90, 180, and 270 degrees
  - The inverse rotations are included here, since -90 == 270, -180 == 180

Algebraically, we write the rotation group as the set

$$\{1, r, r^2, r^3\} \qquad \text{with} \qquad r^4 = 1$$

It has four elements and is called the **Cyclic group of order 4**

Symmetries of a Square: rotations

- So, the rotations of a square give us four transformations
- The identity 1, which is a rotation of 0 degrees (or any multiple of 360)
- The three rotations 90, 180, and 270 degrees
  - The inverse rotations are included here, since -90 == 270, -180 == 180

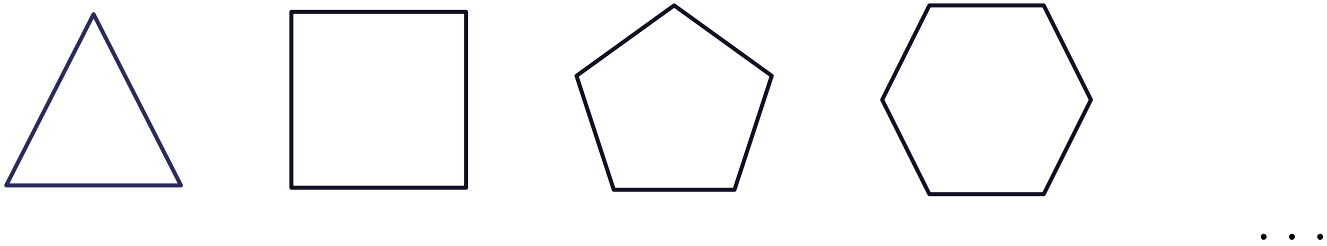
Algebraically, we write the rotation group as the set

$$\{1, r, r^2, r^3\} \qquad \text{with} \qquad r^4 = 1$$

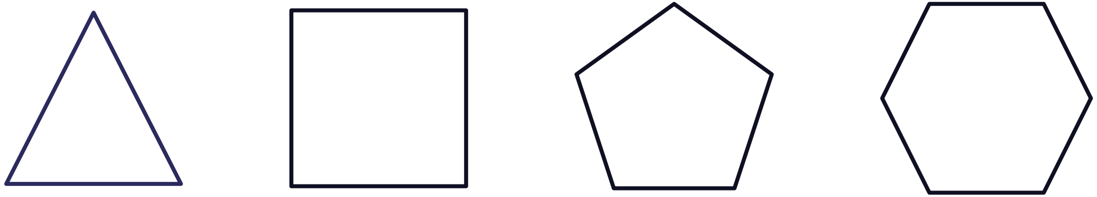
Defn: The **order** of a group is the number of elements

It has four elements and is called the **Cyclic group of order 4**

Cyclic groups: Rotations



Cyclic groups: Rotations

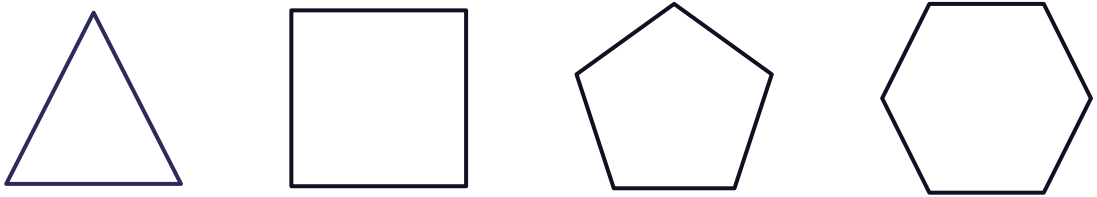


. . .

$r^3 = 1$ $r^4 = 1$ $r^5 = 1$ $r^6 = 1$

120 90 72 60

Cyclic groups: Rotations



$r^3 = 1$ $\quad$ $r^4 = 1$ $\quad$ $r^5 = 1$ $\quad$ $r^6 = 1$

120 $\quad$ 90 $\quad$ 72 $\quad$ 60

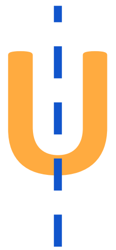
The cyclic group of order n has n elements, generated by a rotation **r** with

$$r^n = 1$$

Cyclic groups of order 2 and 1

- Order 2: need an object with only one (non-identity) symmetry

Letter with one reflection

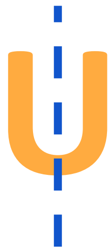


$$r^2 = 1$$

Cyclic groups of order 2 and 1

- Order 2: need an object with only one (non-identity) symmetry
- Order 1: need an object with only the identity symmetry

Letter with one reflection



$$r^2 = 1$$

Letter with no symmetric rotations or reflections

$$r = 1$$

Terminology: Order

- The **order of a group** is the number of elements
  - The cyclic group of order n has n elements

Terminology: Order

- The **order of a group** is the number of elements
    - The cyclic group of order n has n elements

- The **order of an element** is the smallest power which makes it the identity

Terminology: Order

- In the cyclic group of order 6 $r^6 = 1$

$$
\begin{aligned}
|C_6| &= 6 \\
|1| &= 1 \\
|r| &= 6 = |r^{-1}| = |r^5| \\
|r^2| &= 3 = |r^4| \\
|r^3| &= 2
\end{aligned}
$$

Terminology: Order

- In the cyclic group of order 6 $r^6 = 1$

$$
\begin{aligned}
|C_6| &= 6 \\
|1| &= 1 \\
|r| &= 6 = |r^{-1}| = |r^5| \\
|r^2| &= 3 = |r^4| \\
|r^3| &= 2
\end{aligned}
$$

- The order of an element is at most the order of the group
  - In fact, the order of an element is a divisor of the order of the group (Lagrange's theorem)

Cyclic groups: summary

- Groups C_n with the following structure

$$\{1, r, r^2, r^3, \ldots, r^{n-1}\}$$

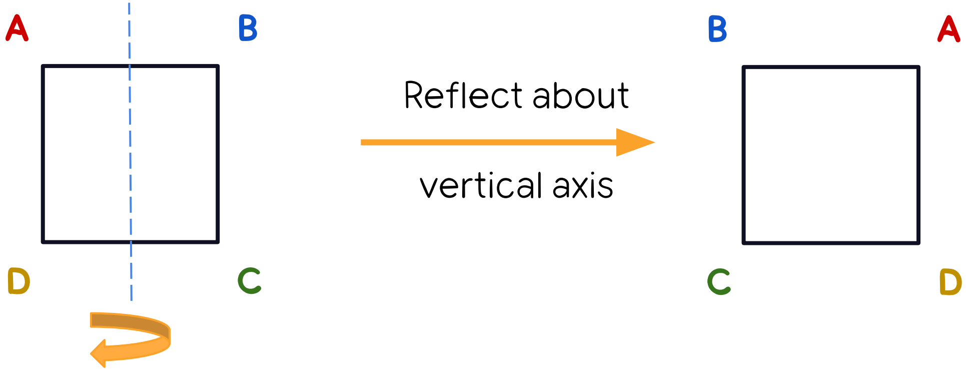
- All ***generated*** by the element r which represents a rotation of 360 / n degrees

- The **generator** r has order n

Dihedral Groups

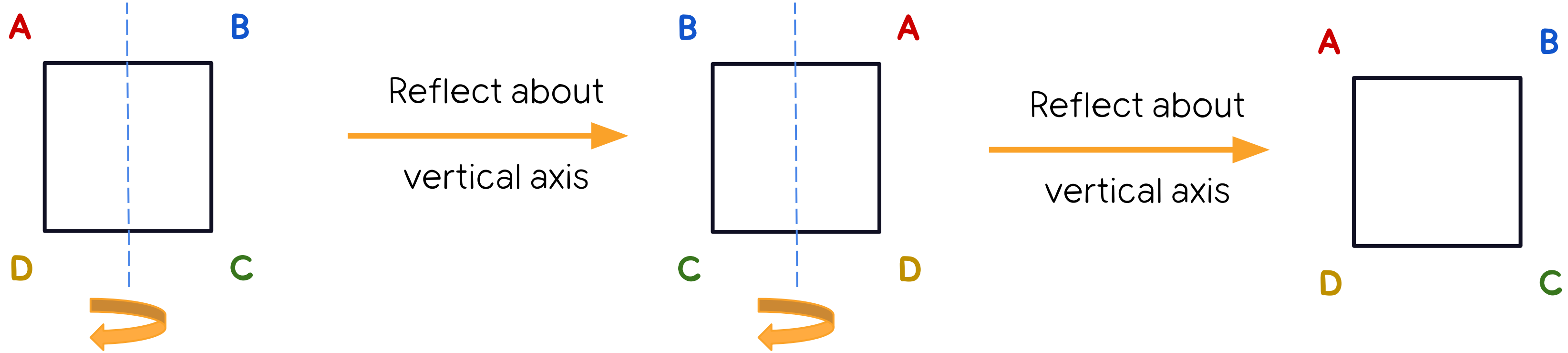
Dihedral groups: rotations + reflections

Squares have reflections as well



Dihedral groups: rotations + reflections

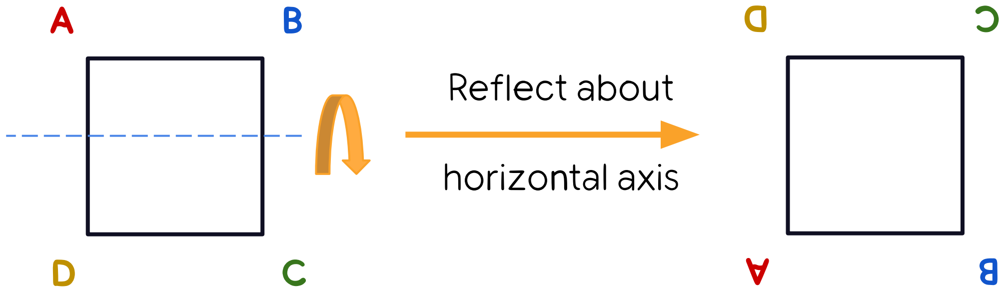
Squares have reflections as well



Call the reflection **s**, then we have that $s^2 = 1$

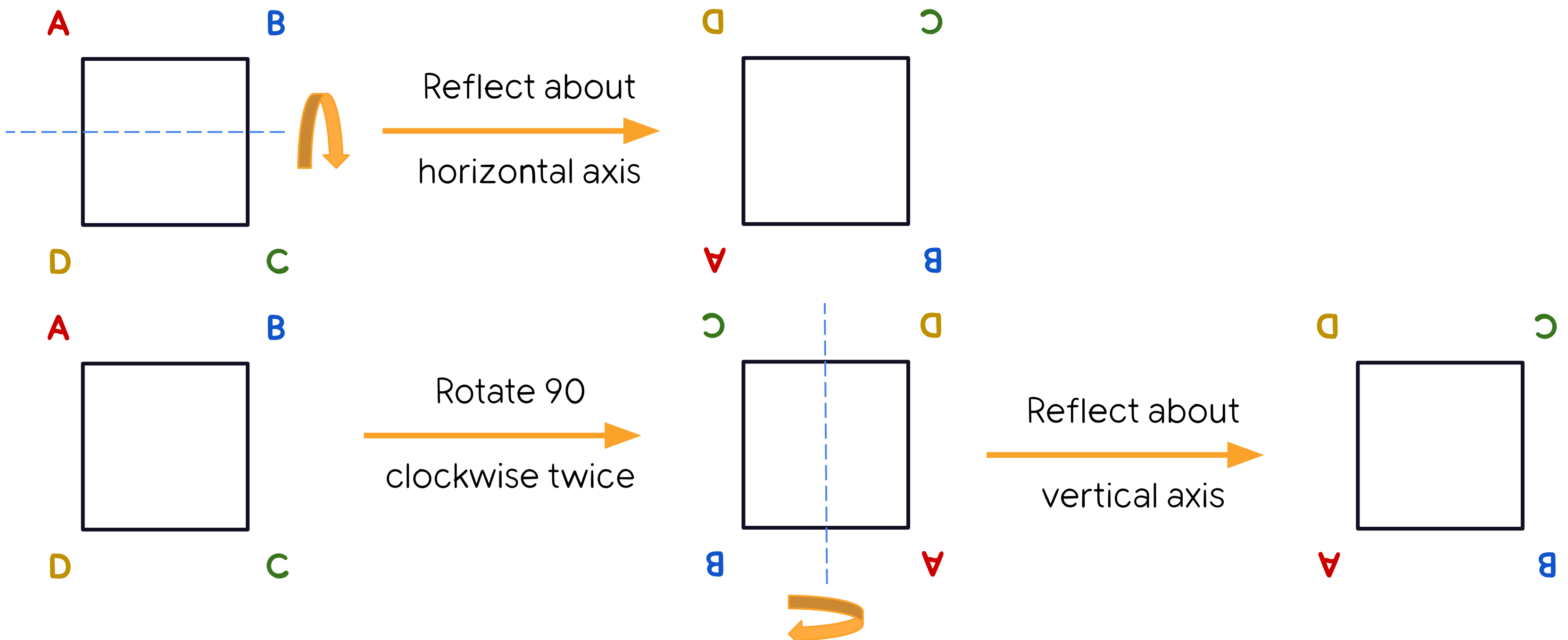
Dihedral groups: rotations + reflections

What about other reflections, say about the horizontal axis?



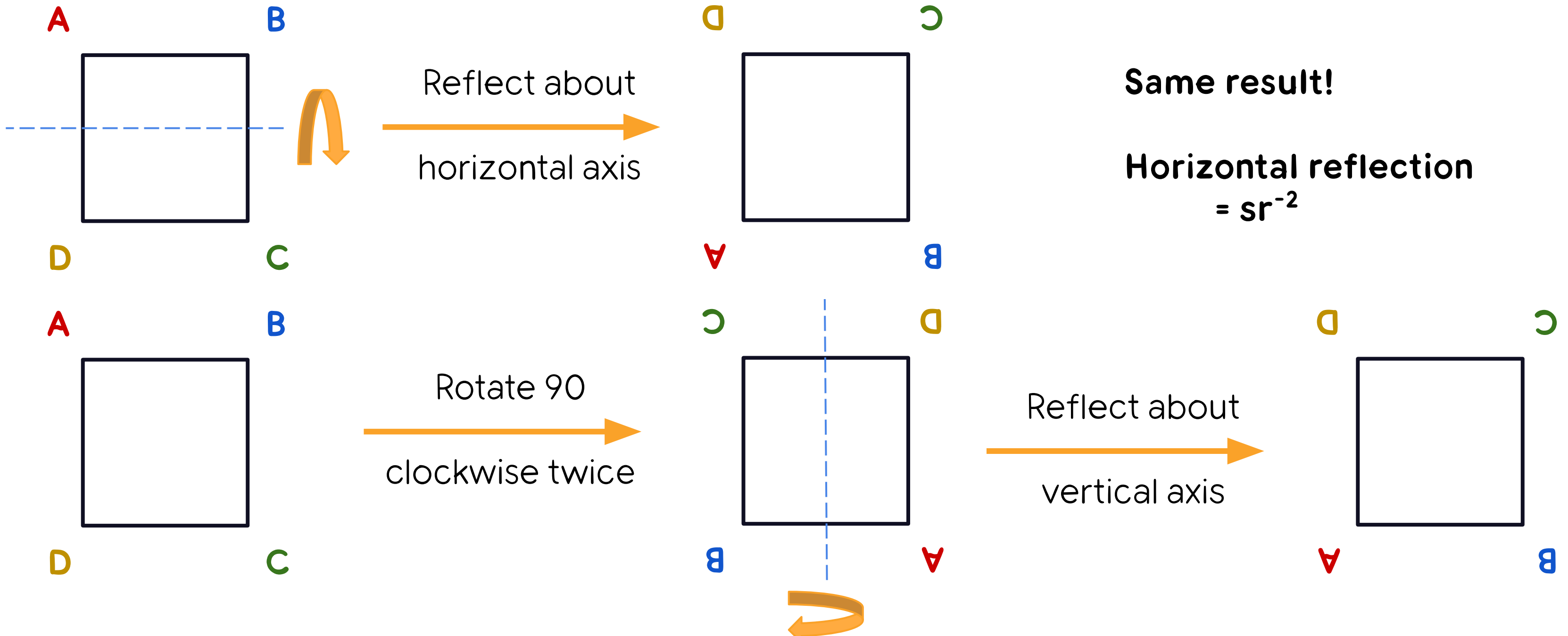
Dihedral groups: rotations + reflections

What about other reflections, say about the horizontal axis?



Dihedral groups: rotations + reflections

What about other reflections, say about the horizontal axis?

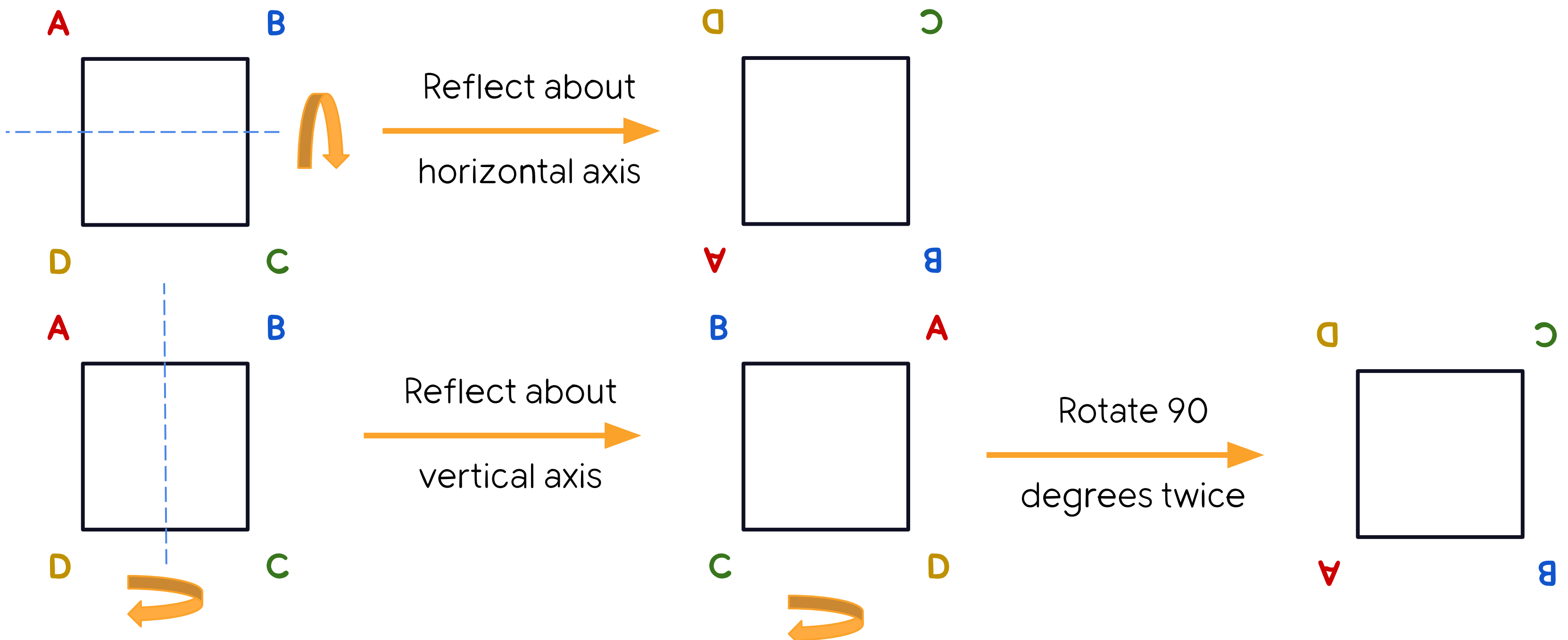


Same result!

Horizontal reflection
$= sr^{-2}$

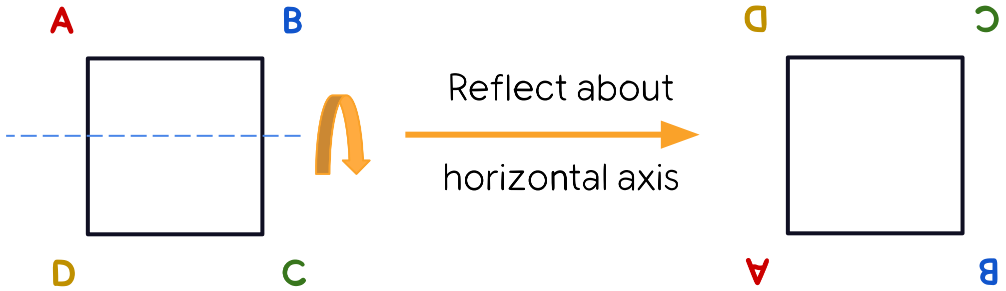
Dihedral groups: rotations + reflections

What about other reflections, say about the horizontal axis?



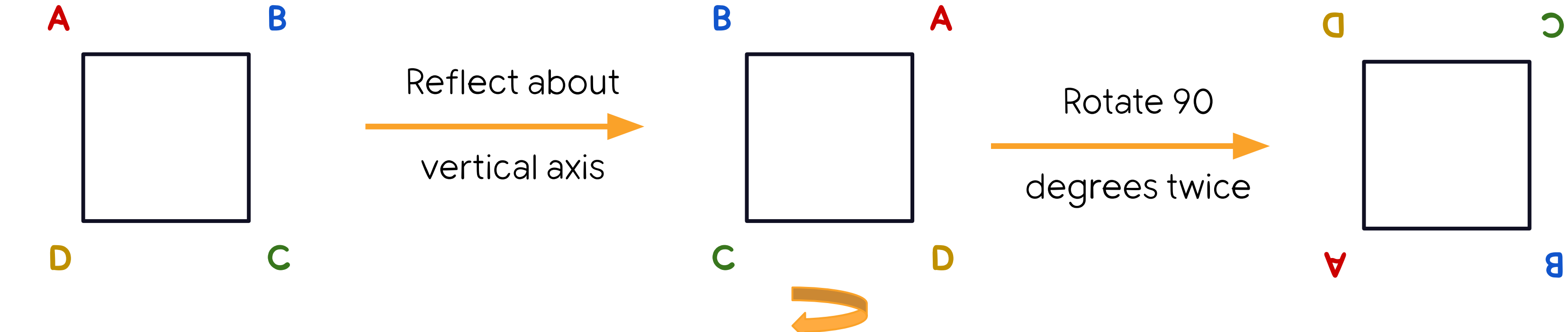
Dihedral groups: rotations + reflections

What about other reflections, say about the horizontal axis?



Same result again!

Horizontal reflection
= r^2s



Dihedral groups: rotations + reflections

- Just need one reflection – all others can be written in terms of **r** and **s**

$$r^k s = s r^{-k}$$

- Full group of rotations and reflections for a square is then just

$$\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

or $\{1, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$

$$r^k s = s r^{-k}$$

Dihedral groups: rotations + reflections

- Just need one reflection – all others can be written in terms of **r** and **s**

$$r^k s = s r^{-k}$$

- Full group of rotations and reflections for a square is then just

$$\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

or $$\{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

$$r^k s = s r^{-k}$$

Note that $rs = sr^{-1}$ which means that r and s do **not** typically commute

Dihedral groups: rotations + reflections

The **dihedral group** of a square is called D_4 and has 8 elements

- It contains the four rotations and the four reflections

Dihedral groups: rotations + reflections

The **dihedral group** of a square is called D_4 and has 8 elements

- It contains the four rotations and the four reflections

More generally, the dihedral group D_n has 2n elements:

- n rotations
- n reflections

Dihedral groups: rotations + reflections

The **dihedral group** of a square is called D_4 and has 8 elements

- It contains the four rotations and the four reflections

More generally, the dihedral group D_n has 2n elements:

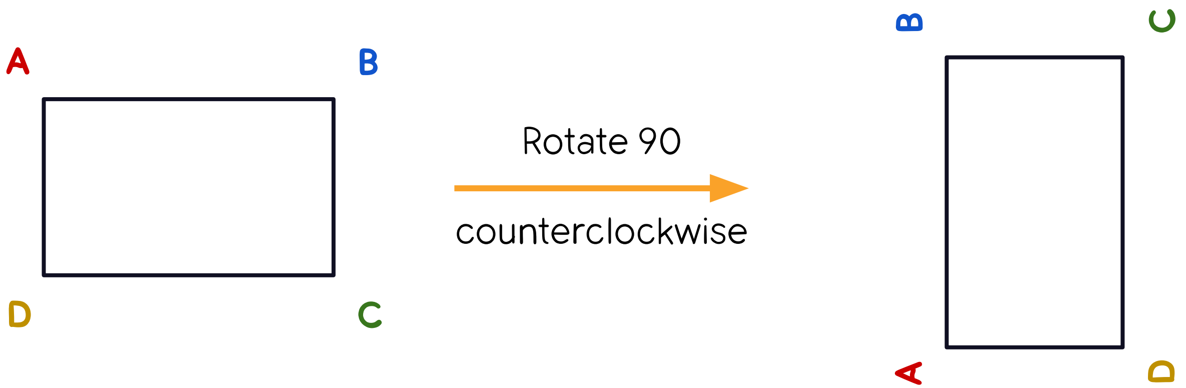
- n rotations
- n reflections

The group is generated by a rotation **r** and a reflection **s**, with the relations

$$r^n = 1$$
$$s^2 = 1$$
$$rs = sr^{-1}$$

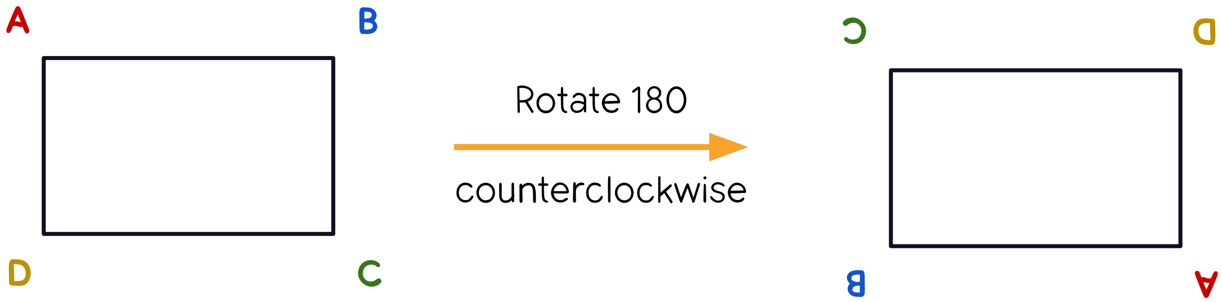
More example groups

Symmetries of a rectangle



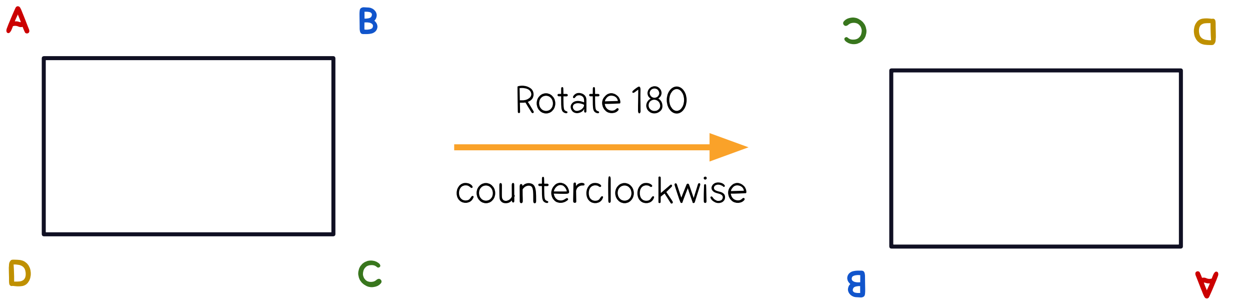
Not a symmetry!

Symmetries of a rectangle

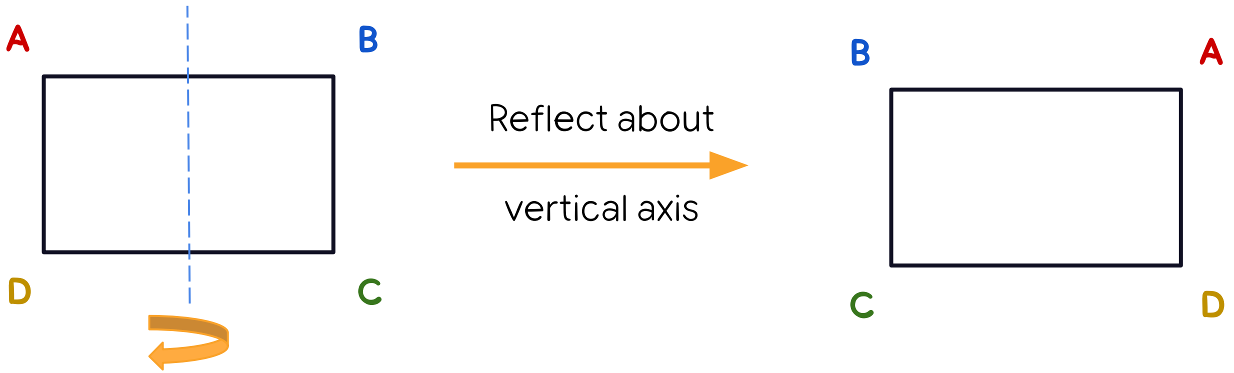


That's better!

Symmetries of a rectangle

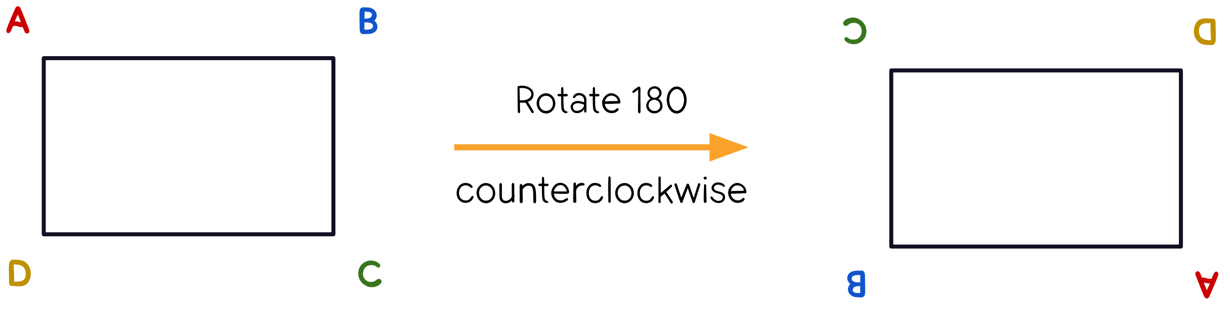


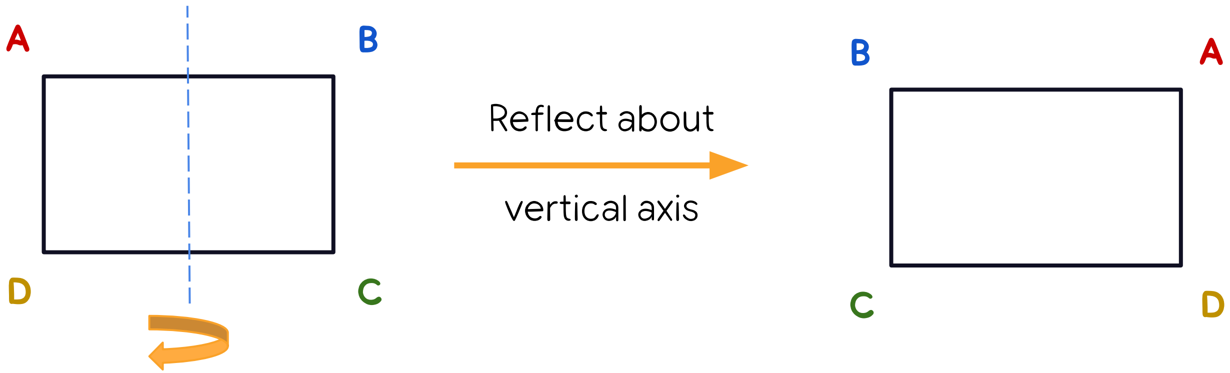
$$r^2 = 1$$



$$s^2 = 1$$

Symmetries of a rectangle

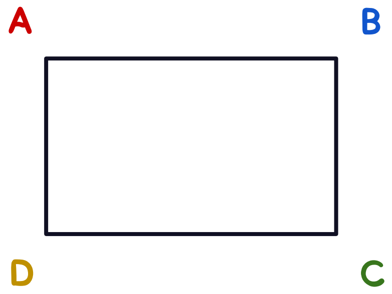




$$r^2 = 1 = s^2 = (rs)^2$$

Symmetries of a rectangle

The group has four elements: **1, r, s, rs** with $r^2 = 1 = s^2 = (rs)^2$



Symmetries of a rectangle

The group has four elements: **1, r, s, rs** with $r^2 = 1 = s^2 = (rs)^2$

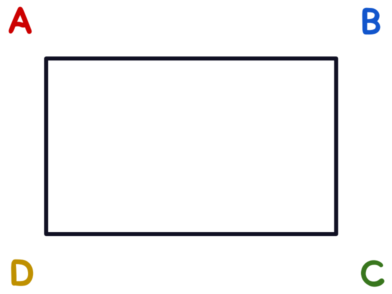
No element of order 4, so it's **not** the cyclic group of order 4!

Symmetries of a rectangle

The group has four elements: **1, r, s, rs** with $r^2 = 1 = s^2 = (rs)^2$

No element of order 4, so it's **not** the cyclic group of order 4!

It's called the **Klein four group**, and is one of the two groups of order 4



Roots of Unity

Solutions of the equation

$$x^n = 1$$

Solutions given by

$$x = e^{\frac{2\pi i}{n}}$$

Roots of Unity

Solutions of the equation

$$x^n = 1$$

Solutions given by

$$x = e^{\frac{2\pi i}{n}}$$

Same as cyclic group of order n!

Technical term: isomorphism

Circle Group: rotations of unit circle

- Rotate by any angle $r_\theta = e^{i\theta}$
- Angles add, modulo 360 $r_\alpha * r_\beta = r_{\alpha+\beta}$

Circle Group: rotations of unit circle

- Rotate by any angle $$r_\theta = e^{i\theta}$$
- Angles add, modulo 360 $$r_\alpha * r_\beta = r_{\alpha+\beta}$$
- This group is infinitely large!
  - Contains all n-th roots of unity and much more
    - So it has elements of all orders
  - Also has elements of infinite order
    - Such as a rotation by an irrational angle

Circle Group: rotations of unit circle

- Rotate by any angle $$r_\theta = e^{i\theta}$$

- Angles add, modulo 360 $$r_\alpha * r_\beta = r_{\alpha+\beta}$$

- This group is infinitely large!
    - Contains all n-th roots of unity and much more
        - So it has elements of all orders
    - Also has elements of infinite order
        - Such as a rotation by an irrational angle

- No single generator of the entire group, so it's not a cyclic group

Groups: Closed collections of symmetries

- Identity group: just one element (cyclic of order 1)
- Single reflection: cyclic of order 2
- Rotations: Cyclic of order n
- All rotations and reflections of regular polygons: Dihedral groups
- Klein four group (symmetry group of rectangle)
- Circle group

Permutation Groups

Permutations: Symmetries of Sets

- Example: encryption substitution ciphers (e.g. ROT13)

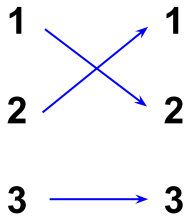
Permutations: Symmetries of Sets

- A permutation is a reversible transformation on the letters of an alphabet
- A given permutation “encrypts” the data. The inverse “decrypts” the data.

Cyclically shifting letters by 3 positions is known as the **Caesar cipher**

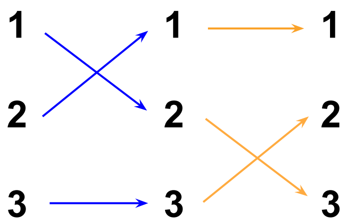
Permutations: Symmetries of Sets

- Composing permutations
- Alphabet: {1, 2, 3}



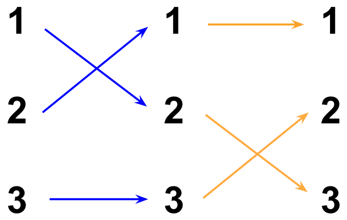
Permutations: Symmetries of Sets

- Composing permutations
- Alphabet: {1, 2, 3}



Permutations: Symmetries of Sets

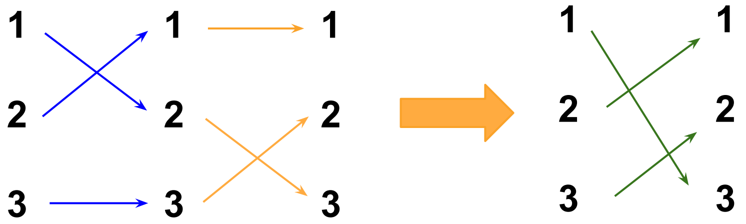
- Composing permutations
- Alphabet: {1, 2, 3}



Both order 2
(self-inverses)

Permutations: Symmetries of Sets

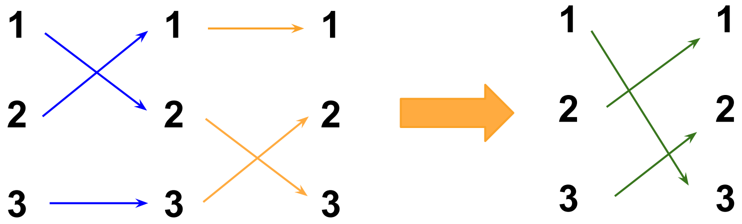
- Composing permutations
- Alphabet: {1, 2, 3}



Both order 2
(self-inverses)

Permutations: Symmetries of Sets

- Composing permutations
- Alphabet: {1, 2, 3}



Both order 2
(self-inverses)

Order 3

Permutations: Symmetries of Sets

- There are cyclic permutations that shift elements in a cycle
  - Such permutations have order n for a set of n elements

1 2 3 4

2 3 4 1

3 4 1 2

4 1 2 3

1 2 3 4

Order 4 permutation

Permutations: Symmetries of Sets

- There are cyclic permutations that shift elements in a cycle
  - Such permutations have order n for a set of n elements

1 2 3 4

2 3 4 1

3 4 1 2

4 1 2 3

1 2 3 4

For a set of n elements, there are permutations of order n

Order 4 permutation

Permutations: Symmetries of Sets

- There are cyclic permutations that shift elements in a cycle
    - Such permutations have order n for a set of n elements

1 2 3 4

2 3 4 1

3 4 1 2

4 1 2 3

1 2 3 4

Order 4 permutation

For a set of n elements, there are permutations of order n

So the cyclic group of order n is contained in the group of permutations on a set of n elements

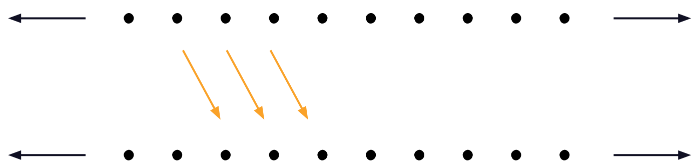
Permutations: Symmetries of Sets

- Among the first groups to be studied
- A set of size n has n! permutations
    - invertible and closed under composition
- The group of permutations on n-elements is called the **Symmetric group** S_n
- Foundational to finite group theory – every finite order group can be represented as a subgroup of a permutation group (Cayley's theorem)

Lattice Groups

Lattice Translations

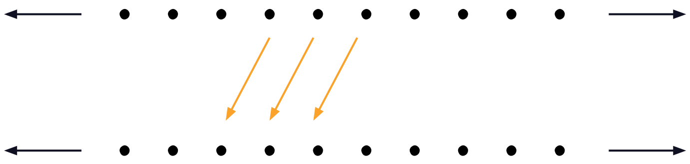
- Translations of a one-dimensional (infinite) lattice



Shift by 1

Lattice Translations

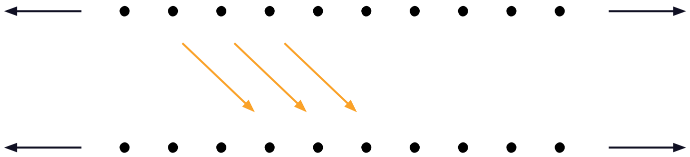
- Translations of a one-dimensional (infinite) lattice



Shift by -1

Lattice Translations

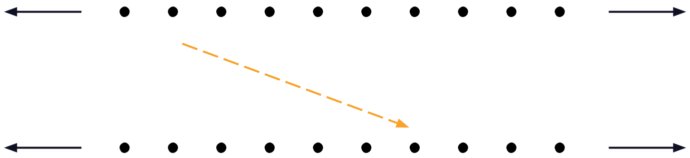
- Translations of a one-dimensional (infinite) lattice



Shift by 2

Lattice Translations

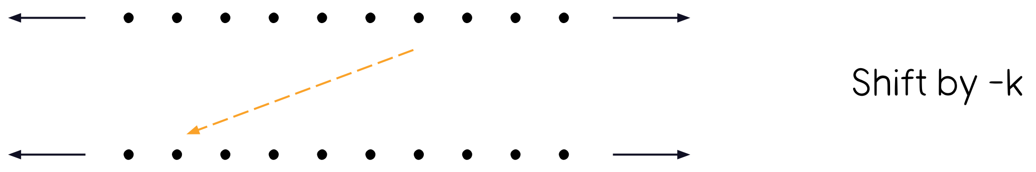
- Translations of a one-dimensional (infinite) lattice
- Can shift by any integer k



Shift by k

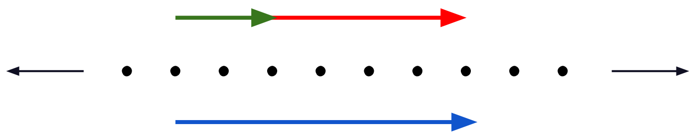
Lattice Translations

- Translations of a one-dimensional (infinite) lattice
- Can shift by any integer k
- Inverse is shift by -k



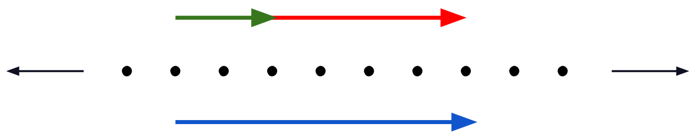
Lattice Translations

- Translations of a one-dimensional (infinite) lattice
- Can shift by any integer k
- Inverse is shift by -k
- Shifts compose by addition
  - Shift by n then m is a shift by n+m



Lattice Translations

- Translations of a one-dimensional (infinite) lattice
- Can shift by any integer k
- Inverse is shift by -k
- Shifts compose by addition
    - Shift by n then m is a shift by n+m
- So the symmetry group of translations is the same as the integers with addition



Abstract Algebra

What’s **abstract** about abstract algebra?

- All the groups we’ve seen are invertible transformations of some object that form a closed collection under composition and inverses

What's **abstract** about abstract algebra?

- All the groups we've seen are invertible transformations of some object that form a closed collection under composition and inverses

- We can define a group abstractly as a set G with:
    - an identity element 1
    - an associative binary operation: for each g, h in G, g * h in G
    - inverses for each element g in G that undo the action of g

Why associative?

What's **abstract** about abstract algebra?

- All the groups we've seen are invertible transformations of some object that form a closed collection under composition and inverses

- We can define a group abstractly as a set G with:
  - an identity element 1
  - an associative binary operation: for each g, h in G, g * h in G
  - inverses for each element g in G that undo the action of g

- Group theory is the study of all abstract objects satisfying these axioms
  - Every group is the set of symmetries of some mathematical object (Frucht's Theorem)

What's next!

- Homework: watch this 3B1B video (~20 mins)
- Next time we'll cover the structure of groups, subgroups, homomorphisms, and related topics

Exercises

Exercise Session Format

- Primarily driven by hands-on examples with calculations, some involving computers (planned for weeks 3 and 4)
- Brief “presentation” section to refresh memory of definitions, concepts, etc.
- Main objective is to illuminate understanding with concrete examples; not meant to be comprehensive in any way
- Exercises emphasize computations and conjectures; we are not doing proofs

Why do exercises?

- Interactivity is essential to learning mathematics
- Working through examples and exercises builds intuition
- Working through non-examples can highlight the essentials of a particular definition or theorem
- Possibly fictional quote attributed to Euclid: “There is no royal road to geometry.”

How hard are the exercises?

- Target audience: Someone who has not taken abstract algebra before
- Exercises are meant to be bite-sized, not time consuming
- If you've taken an abstract algebra class in college before, the exercises will likely be very easy

Other Resources

Beyond these lectures and exercise sessions, you can keep learning algebra by...

- Finding a few colleagues interested in learning with you
- Asking the instructors some questions
- Take a college class
- Reading:
    - Gallian's *Contemporary Abstract Algebra*
    - Artin's *Algebra*
    - Dummit and Foote's *Abstract Algebra*
    - Herstein's *Abstract Algebra*

Agenda

- Review definition of a group
- Give examples and non-examples of groups
- Go in-depth and do calculations with certain groups:
  - Integers mod n
  - Dihedral group
  - Symmetric group (if we have time)

Definition of a group

A ***group*** is a set G together with a binary operation (the “group operation”) $*: G \times G \to G$ which satisfies:

- **Associativity**: for all $g_1, g_2, g_3 \in G$, $(g_1 * g_2) * (g_3) = g_1 * (g_2 * g_3)$
- **Existence of identity:** there exists an element $e \in G$ such that for all $g \in G$, $(e * g) = (g * e) = g$.
- **Existence of inverses:** for every element $g \in G$, there exists an element $g^{-1} \in G$ such that $(g * g^{-1}) = (g^{-1} * g) = e$.

How do we “describe” a specific group?

The group definition is very abstract. What are examples of specific groups, and how do we describe them?

- As a familiar mathematical object
    - eg, integers, rationals, or reals under addition, certain subsets of matrices under matrix multiplication
- By explicitly writing out a multiplication table
- Other abstract ways, such as a “group presentation”

Example: $(\mathbb{Z}, +)$ - the integers under addition

$(\mathbb{Z}, +)$ forms a group:

- addition is associative
- 0 is the identity
- The inverse of 1 is -1, and more generally the inverse of a is $-a$.

You can also see that the above logic extends to rationals ($\mathbb{Q}$), reals ($\mathbb{R}$), or complex numbers ($\mathbb{C}$) under addition.

(Recall: a ***rational number*** is a number in the form a/b, where a, b are integers, and b is not zero).

Non-example: $(\mathbb{Z}, *)$ - the integers under multiplication

In contrast, $(\mathbb{Z}, *)$ does not form a group. For example, most integers do not have multiplicative inverses which are also integers.

- $(\mathbb{Q}, *)$ is not a group either (why?)
- However, what about non-zero rationals under multiplication?
    - What is the identity?
    - Does each element have an inverse?
    - What about non-zero reals or complex numbers?
- Notation: $\mathbb{Q}^*$ = non-zero rationals

Non-example: odd integers under addition

Arbitrary subsets of groups are generally not groups either.

Example: odd integers under addition…

- + is associative, but
- odd integers aren't even ***closed*** under addition (that is, if x, y are odd, x+y is not always odd)
- there is no identity

Examples: even integers under addition

… but sometimes subsets are groups!

Example: even integers under addition

- $+$ is associative, but
- 0 is even, hence the even integers have the identity
- if a and b are even, so is $a + b$
- if a is even, so is $-a$.

The even integers form an example of a **subgroup** of the integers.

(Homework: Can you describe all subsets of integers that are a group under $+$?)

Integers mod n

Motivation: Addition on a clock

Consider a standard 12-hour clock.

An event starts at 10AM. It takes 5 hours. What time does it end?

- 15 AM? No… there's no 15 AM.
- 3 PM!
- You calculated this by computing $10 + 5 - 12 = 3$.

This is an example of *addition mod 12*, an addition system where all sums are less than 12.

Integers mod n: a definition

Consider the integers {0, 1, 2, … n−1}, with the binary operation of “clock” addition or “remainder by n”: if a + b >= n, “define” a + b to be a + b − n. This forms a group called the “integers mod n” and are denoted $\mathbb{Z}_n$.

- Example: Let n = 3. Then:
  - 1 + 1 = 2,
  - 2 + 1 = 0,
  - 2 + 2 = 1.
- To distinguish between addition of ordinary integers vs. integers mod n, one notation is to write $[1]_3$ for 1 in $\mathbb{Z}_3$.
- We write a ≡ b mod n to mean n divides (a−b).
- This is a group! (What is the identity? Convince yourself inverses exist.)

Exercises: Integers mod n under multiplication

Consider $\mathbb{Z}_n$ but this time with multiplication instead of addition.
This is not a group because 0 has no inverse.
Suppose we remove 0.

Exercise: Formulate a conjecture as to when $\mathbb{Z}_n - \{0\}$ under multiplication is a group. (Optional homework: prove your conjecture)
(To see a pattern, work through some examples for small values of n, like n = 2, 3, 4, 5).

Exercise. For general n, can you describe the largest subset of $\mathbb{Z}_n$ which forms a group under multiplication?

Example: $\{[1]_4, [3]_4\}$ is a group under multiplication, and is the largest such group for n=4, because no other elements have multiplicative inverses mod 4.

Exercise: Primitive roots mod p

Let p = a prime number.

Exercise. For small values of p (p = 7, 11, ...), can you find a **generator** for $\mathbb{Z}_p^*$? That is, can you find a single element $[x]_p$ of $\mathbb{Z}_p^*$ such that every element of $\mathbb{Z}_p^*$ can be written as $([x]_p)^k$ for some integer k?

Example: in $\mathbb{Z}_3^*$, $[2]_3$ is a generator: $([2]_3)^2 = [1]_3$.
In $\mathbb{Z}_5^*$, $[2]_5$ is a generator, but $[4]_5$ is not.

A generator for $\mathbb{Z}_p^*$ is called a **primitive root mod p**.

Exercise. For what value(s) of p are primitive roots unique?

Facts and open questions about primitive roots

Every $\mathbb{Z}_p^*$ has a primitive root. (Homework:: how many are there?) This fact is fairly easy to prove (though we do not do it here).

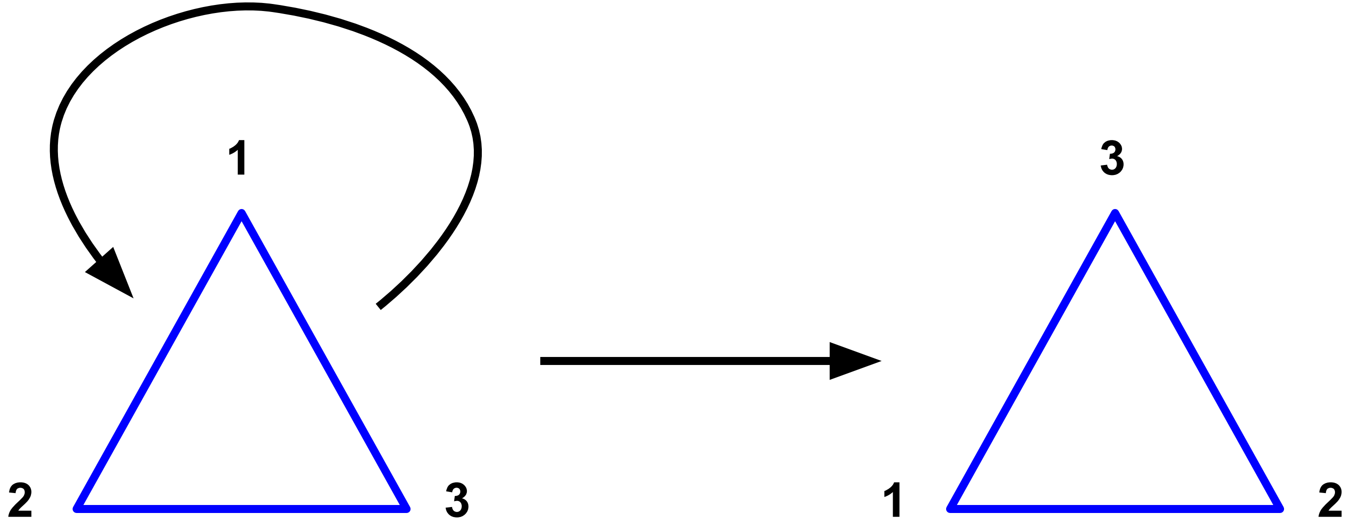
What is the most efficient algorithm for finding a primitive root? This is an open question!

Suppose *a* is an integer, is not a square, and is not –1. Is *a* a primitive root mod p for infinitely many primes *p*? This is an open question! (Artin's conjecture) (Homework: why are the restrictions "not a square" and "not –1" required?)

Dihedral Groups: Symmetries of regular polygons

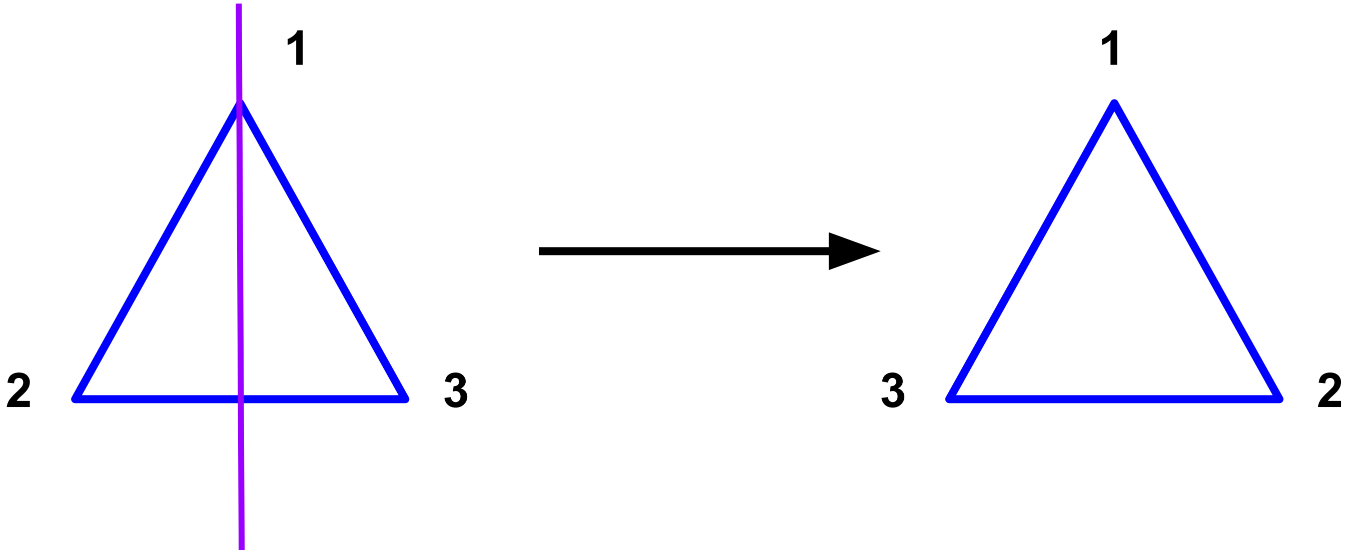
Example: plane symmetries of a regular triangle

Consider an equilateral triangle which lies in the plane. It has some symmetries:
(counterclockwise) Rotation by 120 degrees:



Reflection of a triangle

Reflection across the vertical axis:



Exercise: Let's explore the symmetries of a triangle

- How many symmetries of an equilateral triangle are there? Can you prove this? Draw diagrams like in the previous few slides for each symmetry.
- Convince yourself they form a group under composition (if g_1, g_2 are symmetries, $g_1 * g_2$ is the symmetry obtained by applying g_2 and then g_1)
  - eg, rotation by 120 degrees * rotation by 120 degrees = rotation by 240 degrees
  - What is the identity element?
  - What are the inverse elements of each element?
  - Give names to each element. Can you write down a "multiplication table" for these elements? (If you get bored after filling in half the entries it's fine to stop early)

Some standard mathematical notation for symmetries of a regular polygon

The group of symmetries of an equilateral triangle is called the **dihedral group with 6 elements**, and is written D_3 (sometimes D_6).

- Rotation by 120 degrees is often named “r” (rotation)
- Reflection across some axis (say the vertical axis) is often named “s”.

This is all naturally generalizable to regular n-gons, and their symmetry group is written D_n.

Exercise: Group operations in D_3

How are r, s related to each other? In particular:

- What happens when you multiply r by itself repeatedly? What about s?
- Convince yourself that $rs \neq sr$. Does $rs = sr^i$ for some value of i? Draw diagrams illustrating how rs vs. sr act on a triangle that show this.

Check that every element of D_3 can be uniquely written in the form $s^i r^j$, where $i = 0$ or 1, $j = 0, 1,$ or 2.

Say you multiply two elements of the above form together. (eg, $(sr) * (sr^2)$) How can you convert this product to the form $s^i r^j$?

Homework exercise

Verify that D_n is a group (at the least, try enumerating elements of symmetries of a square or regular hexagon and convincing yourself they satisfy group axioms).

What are the analogous equations to those on the previous slide for D_{2n}? Can you find an explicit description of every element of D_{2n} as a product of various numbers of r, s?

$\mathbb{Z}_n$ inside D_n

Suppose you multiply r by itself repeatedly. You end up with the subset $\{1, r, r^2, \ldots, r^{n-1}\}$ inside of D_n.

Also, note that:

- $r^i * r^j = r^{i+j}$,
- and if $i + j > n$, then $r^i * r^j = r^{i+j-n}$.

In other words: the exponents of r behave exactly like elements of $\mathbb{Z}_n$!

Symmetric Group: Permutations of a finite set

Permutations: Definition

Consider a finite set S, which we will just label with positive integers, like {1, 2, ..., n}. A permutation is a rearrangement of the integers in S.

Example: $n = 3$. The rearrangement $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1$ is a permutation, but the function $1 \rightarrow 2, 2 \rightarrow 2, 3 \rightarrow 3$ is not, because both 1, 2 go to 2.

More formally,

A **permutation** of S is a function $p: S \rightarrow S$ which is

- 1 to 1: if $p(x) = p(y)$, then $x = y$. In other words, distinct elements map to distinct elements.
- surjective: for every y, there exists some x such that $p(x) = y$.

Group of Permutations

Suppose n is a fixed positive integer. The set of permutations of $\{1, 2, ..., n\}$ is denoted S_n, and form a group under function composition. (Homework: check group axioms!)

Example: S_2 has two elements: the permutations p_1, p_2, where $p_1(1) = 1$, $p_1(2) = 2$, and $p_2(1) = 2$ and $p_2(2) = 1$. p_1 is the identity, and $p_2 \circ p_2 = p_1$.

The group S_n is called the **symmetric group** on n elements.

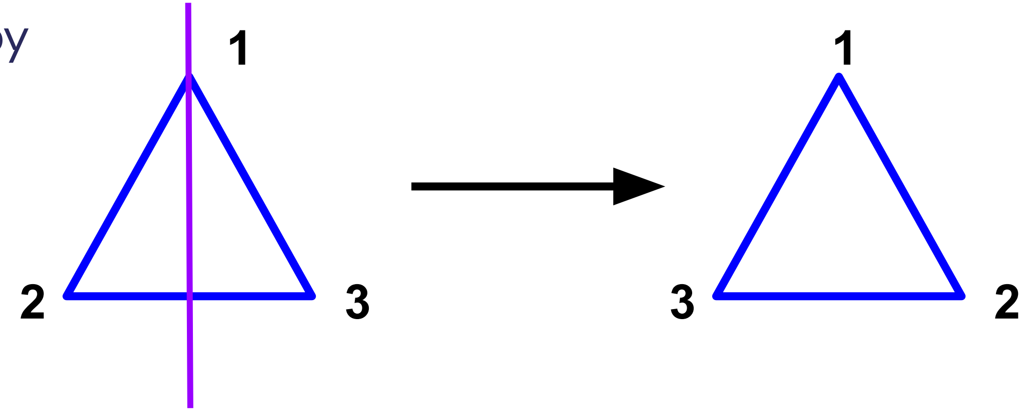
You can think of a permutation as a "symmetry" of $\{1, 2, ..., n\}$, in that a permutation keeps $\{1, 2, ..., n\}$ invariant.

A connection with dihedral groups

Think back to D_3, the symmetries of an equilateral triangle.

If we label the vertices of the triangle with 1, 2, 3, then each element of D_3 can be thought of as a permutation of {1, 2, 3}, depending on how the symmetry rearranges the vertices. For example:

the element of D_3 represented by the diagram on the right can be thought of as the permutation swapping 2 and 3 (and keeping 1 fixed).



Exercises: D_3 vs. S_3

Exercise: Show that D_3 and S_3 are identical groups, in the sense that exists a bijection (1–1 and surjective, like a permutation) $f: D_3 \rightarrow S_3$ which preserves group structure, ie, $f(g*h) = f(g) * f(h)$ for every pair of elements $f, g \in D_6$.

- What is f(id)?
- How are $f(r)$ and $f(r^{-1})$ related? More generally, how are $f(g)$ and $f(g^{-1})$ related, for an arbitrary g?
- Is this group-preserving map f unique?
- What if you try to do something similar with D_4 and S_4?

Appendix

An aside: Abelian groups

Notice that addition in $\mathbb{Z}_n$ is commutative. If a group G has a commutative binary operation (that is, $gh = hg$ for all $g, h \in G$), we call G an **abelian group**.

In contrast, notice that D_{2n}, S_n $(n > 2)$ are not abelian.

Permutations: Notation

In group theory, “cycle notation” is a common way of compactly writing down individual permutations. A **cycle** $(s_1\ s_2\ \ldots\ s_k)$ represents a permutation p which satisfies $p(s_i) = s_{i+1}$, $p(s_k) = p_1$. For integers j which are not present in the cycle, $p(j) = j$.

Examples:

- The identity map has no non-trivial cycles, so we write it as 1.
- The unique non-identity element of S_2 is (1 2).
- The elements of S_3 are 1, (1 2), (1 3), (2 3), (1 2 3), (1 3 2).
- Some permutations are products of cycles. For example, (1 2) (3 4) in S_4 or (1 3)(2 4).

Basic calculations with cycles

Cycle notation makes it easy to write down inverses: just reverse the order in each cycle.

Example: $(1\ 3\ 2\ 5\ 4)^{-1} = (1\ 4\ 5\ 2\ 3)$.

Products of cycles are a little harder to compute. Examples:

- $(1\ 2)(1\ 3) = (1\ 3\ 2)$. To see this: $(1\ 2)(1\ 3)\ 1 = (1\ 2)\ 3 = 3$, $(1\ 2)(1\ 3)\ 2 = (1\ 2)\ 2 = 1$, $(1\ 2)(1\ 3)\ 3 = (1\ 2)\ 1 = 2$.
- $(1\ 2\ 3)(2\ 4) = (1\ 2\ 4\ 3)$.