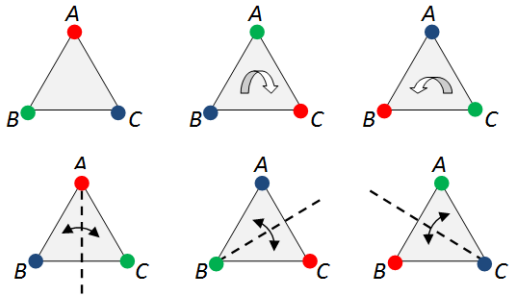
Ma/CS 6a

Class 19: Isomorphisms and Subgroups



By Adam Sheffer

Reminder: A Group

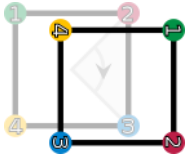
- A group consists of a set G and a binary operation $*$, satisfying the following.
  - **Closure.** For every $x, y \in G$, we have $x * y \in G$.
  - **Associativity.** For every $x, y, z \in G$, we have $(x * y) * z = x * (y * z)$.
  - **Identity.** The exists $e \in G$, such that for every $x \in G$, we have $e * x = x * e = x$.
  - **Inverse.** For every $x \in G$ there exists $x^{-1} \in G$ such that $x * x^{-1} = x^{-1} * x = e$.

Reminder: What We Already Know About Groups

- Given a group with a set G:
  - The multiplication table of G is a Latin square.
  - The identity is unique.
  - For each $a \in G$, there is a unique inverse a^{-1}.
  - For $a, b \in G$, the equation $ax = b$ has a unique solution.

Reminder: Orders

- The order of a group is the number of elements in its set G.
- The *order of an element* $a \in G$ is the least positive integer k that satisfies $a^k = 1$.



Rotation $90°$

4

$\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$

(under multiplication mod 3)

2

$\boxed{5}$

(under integer addition)

∞

Reminder: A Group of 2×2 Matrices

- 2×2 matrices of the form

$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$$

where $\alpha \in \{1,2\}$ and $\beta \in \{0,1,2\}$.

- The operation is matrix multiplication $mod\ 3$.
- The group is of order 6:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

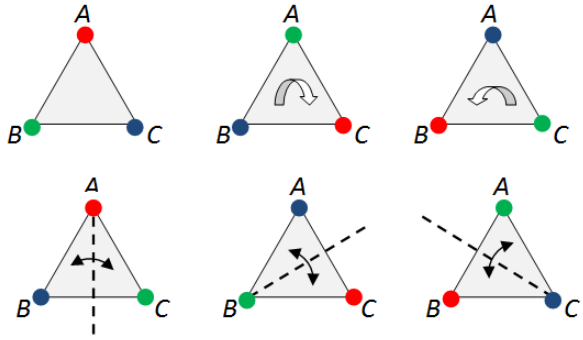
The Multiplication Table

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$
$$X = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \quad Z = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

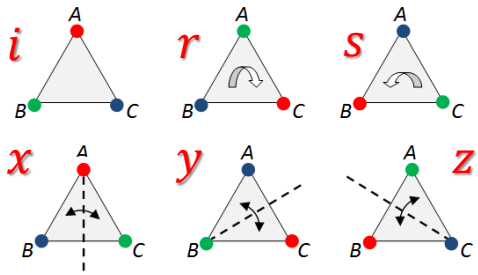
	I	*R*	*S*	*X*	*Y*	*Z*
I	*I*	*R*	*S*	*X*	*Y*	*Z*
R	*R*	*S*	*I*	*Y*	*Z*	*X*
S	*S*	*I*	*R*	*Z*	*X*	*Y*
X	*X*	*Z*	*Y*	*I*	*S*	*R*
Y	*Y*	*X*	*Z*	*R*	*I*	*S*
Z	*Z*	*Y*	*X*	*S*	*R*	*I*

Symmetries of a Triangle

- The six symmetries of the triangle form a group (under composition).



Another Multiplication Table



	i	*r*	*s*	*x*	*y*	*z*
i	*i*	*r*	*s*	*x*	*y*	*z*
r	*r*	*s*	*i*	*y*	*z*	*x*
s	*s*	*i*	*r*	*z*	*x*	*y*
x	*x*	*z*	*y*	*i*	*s*	*r*
y	*y*	*x*	*z*	*r*	*i*	*s*
z	*z*	*y*	*x*	*s*	*r*	*i*

	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	y	z	x
s	s	i	r	z	x	y
x	x	z	y	i	s	r
y	y	x	z	r	i	s
z	z	y	x	s	r	i

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

Isomorphisms

- G_1, G_2 – two groups of the same order.
- A bijection $\beta: G_1 \to G_2$ is an ***isomorphism*** if for every $a, b \in G_1$, we have
$$\beta(ab) = \beta(a)\beta(b).$$
(i.e., after reordering, we have the same multiplication tables)

- When such an isomorphism exists, G_1 and G_2 are said to be ***isomorphic***, and write $G_1 \approx G_2$.

Isomorphism Over the Reals

- **Problem.** Prove that the following groups are isomorphic:
  - The set of real numbers $\mathbb{R}$ under addition.
  - The set of positive real numbers $\mathbb{R}^+$ under multiplication.
- **Proof.**
  - Use the functions $e^x: \mathbb{R} \to \mathbb{R}^+$ and $\log x: \mathbb{R}^+ \to \mathbb{R}$ as bijections between the two sets.
  - For $x, y \in \mathbb{R}$ we have $e^x e^y = e^{x+y}$.
  - For $x, y \in \mathbb{R}^+$, we have $\log x + \log y = \log xy$.

Isomorphism Between $\mathbb{Z}_4$ and $\mathbb{Z}_5^+$

- **Problem.** Are the following two groups isomorphic?
  - The set $\mathbb{Z}_4 = \{0,1,2,3\}$ under addition $mod\ 4$.
  - The set $\mathbb{Z}_5^+ = \{1,2,3,4\}$ under multiplication $mod\ 5$.
- **Solution.**
  - Yes. Use the following bijection of $\mathbb{Z}_4 \leftrightarrow \mathbb{Z}_5^+$.

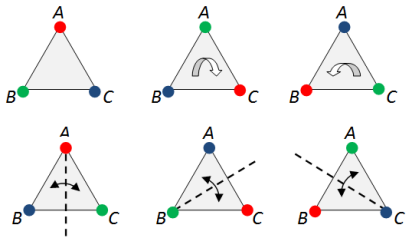
$$0 \leftrightarrow 1$$
$$1 \leftrightarrow 2$$
$$2 \leftrightarrow 4$$
$$3 \leftrightarrow 3$$

Cyclic Groups

- A group G is *cyclic* if there exists an element $x \in G$ such that every member of G is a power of x.
- We say that x *generates* G.
- What is the order of x? $|G|$.
- An infinite group G is cyclic if there exists an element $x \in G$ such that
  $G = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, x^3, \dots\}$

Cyclic Groups?

- Are the following groups cyclic?
  - Integers under addition.
    - Yes! It is generated by the integer 1 (which is not the identity element).
  - The symmetries of the triangle.
    - No. There are no generators.



Cyclic Groups?

- Are the following groups cyclic?
  - The positive reals $\mathbb{R}^+$ under multiplication.
    - No. For example, nothing can generate 1.
  - The aforementioned group of elements of the form $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$.
    - No. Because it is isomorphic to the triangle symmetry group.

Finite Cyclic Groups

- Any cyclic group of a finite order m with *generator* g can be written as
$$\{1, g, g^2, \dots, g^{m-1}\}.$$
- For integers q and $0 \leq r < m$, we have $g^{qm+r} = g^r$.
- Where did we already encounter such a group?
  - Integers $mod\ m$ under addition.
  - The generator is 1 and the group is $\{0,1,2, \dots, m-1\}$.

Isomorphic Cyclic Groups

- **Claim.** All of the cyclic groups of a finite order m are isomorphic. We refer to this group as C_m.
- **Proof.** Consider two such cyclic groups
$$G_1 = \{1, g, g^2, g^3, \dots, g^{m-1}\},$$
$$G_2 = \{1, h, h^2, h^3, \dots, h^{m-1}\}.$$
  - Consider the bijection $\beta: G_1 \to G_2$ satisfying $\beta(g^i) = h^i$.
  - This is an isomorphism since
$\beta(g^i g^j) = \beta(g^{i+j}) = h^{i+j} = h^i h^j = \beta(g^i)\beta(g^j)$.

Simple Groups

- A *trivial group* is a group that contains only one element – an identity element.
- A *simple group* is a non-trivial group that does not contain any other "well-behaved" *subgroups* in it.
- The finite simple groups are, in a certain sense, the "basic building blocks" of all finite groups.
  - Somewhat similar to the way prime numbers are the basic building blocks of the integers.

Classification of Finite Simple Groups

- "*One of the most important mathematical achievements of the 20th century was the collaborative effort, taking up more than 10,000 journal pages*" (Wikipedia).
- Written by about 100 authors!
- **Theorem.** Every finite simple group is isomorphic to one of the following groups:
  - A cyclic group.
  - An alternating group.
  - A simple Lie group.
  - One of the 26 sporadic groups.

The Monster Group

- One of the 26 sporadic groups is the *monster group*.
- It has an order of 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.
- The 6 sporadic groups that are not "contained" in the *monster group* are called *the happy family*.

Direct Product

- G_1, G_2 - two groups with identities $1_1, 1_2$.
- The *direct product* $G_1 \times G_2$ consists of the ordered pairs (a, b) where $a \in G_1$ and $b \in G_2$.
- The direct product is a group:
  - The group operation is
    $$(a, b)(c, d) = (ac, bd).$$
  - The identity element is $(1_1, 1_2)$.
  - The inverse $(a, b)^{-1}$ is (a^{-1}, b^{-1}).
  - The order of $G_1 \times G_2$ is $|G_1||G_2|$.

Direct Product Example

- **Problem.** Is C_6 isomorphic to $C_2 \times C_3$?
- **Solution.**
  - Write $C_2 = \{1, g\}$ and $C_3 = \{1, h, h^2\}$.
  - Then $C_2 \times C_3$ consists of
    $\{(1,1), (1, h), (1, h^2), (g, 1), (g, h), (g, h^2)\}$.
  - $C_2 \times C_3$ is isomorphic to C_6 iff it is cyclic.
  - It is cyclic, since it is generated by (g, h).

$$(g,h)^1 = (g,h), \quad (g,h)^2 = (1,h^2),$$
$$(g,h)^3 = (g,1), \quad (g,h)^4 = (1,h),$$
$$(g,h)^5 = (g,h^2), \quad (g,h)^6 = (1,1),$$

Another Direct Product Example

- **Problem.** Is C_8 isomorphic to $C_2 \times C_4$?
- **Solution.**
  - Write $C_2 = \{1, g\}$ and $C_4 = \{1, h, h^2, h^3\}$.
  - Then $C_2 \times C_4$ consists of $\{(1,1), (1,h), (1,h^2), (1,h^3), (g,1), (g,h), (g,h^2), (g,h^3)\}$.
  - $C_2 \times C_4$ is isomorphic to C_8 iff it is cyclic.
  - It is not. The orders of the elements are 1,4,2,4,2,4,2,4, respectively.

Cyclic Inner Products of Cyclic Groups

- **Claim.** If m, n are relatively prime positive integers, then $C_m \times C_n \approx C_{mn}$.
- **Proof.** Write $C_m = \{1, g, g^2, \ldots, g^{m-1}\}$ and $C_n = \{1, h, h^2, \ldots, h^{n-1}\}$.
  - It suffices to prove that (g, h) generates $C_m \times C_n$.
  - $(g,h)^k = (1,1)$ if and only if $m|k$ and $n|k$.
  - Recall: $\mathrm{GCD}(m,n) = 1$ implies $\mathrm{LCM}(m,n) = mn$.
  - Thus, the order of (g,h) is mn.

Cyclic Inner Products of Cyclic Groups

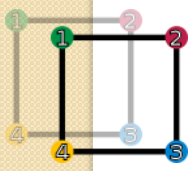
- **Claim.** If m, n are relatively prime positive integers, then $C_m \times C_n \approx C_{mn}$.
- **Proof.** Write $C_m = \{1, g, g^2, \dots, g^{m-1}\}$ and $C_n = \{1, h, h^2, \dots, h^{n-1}\}$.
  - We proved that (g, h) is of order mn.
  - It remains to show that for every $0 \leq i < j < mn$, we have $(g, h)^i \neq (g, h)^j$.
  - If $(g, h)^i = (g, h)^j$, multiplying both sides by $(g, h)^{-i}$ implies $(g, h)^{j-i} = (1,1)$.
  - *Contradiction to the order of* (g, h)*!* So (g, h) generates mn distinct elements.

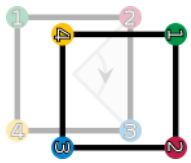
Subgroups

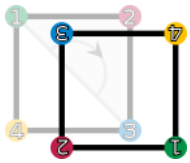
- A *subgroup* of a group G is a group with the same operation as G, and whose set of members is a subset of G.
- Find a subgroup of the group of integers under addition.
  - The subset of even integers.
  - The subset $\{\dots, -2r, -r, 0, r, 2r, \dots\}$ for any integer $r > 1$.

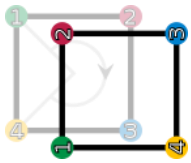
Subgroups of a Symmetry Group

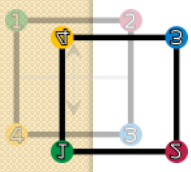
- **Problem.** Find a subgroup of the symmetries of the square.

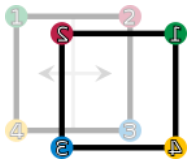

No action

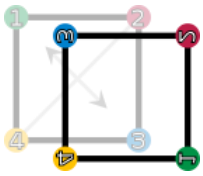

Rotation 90°

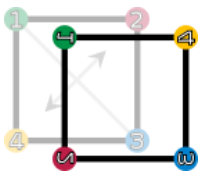

Rotation 180°


Rotation 270°


Vertical flip

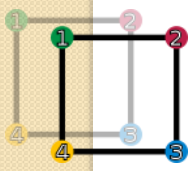

Horizontal flip

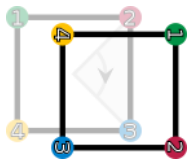

Diagonal flip

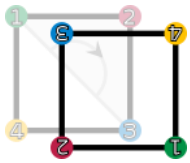

Diagonal flip 2

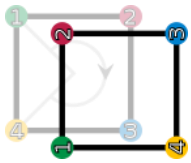
Subgroups of a Symmetry Group

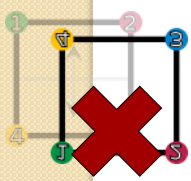
- **Problem.** Find a subgroup of the subgroup.

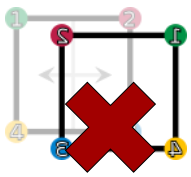

No action

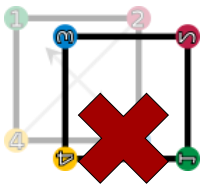

Rotation 90°

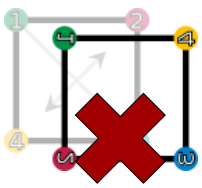

Rotation 180°


Rotation 270°

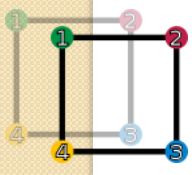

Vertical flip


Horizontal flip

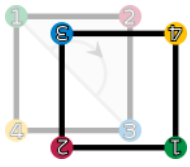

Diagonal flip

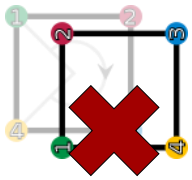

Diagonal flip 2

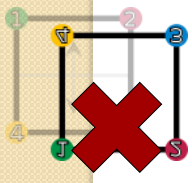
Subgroups of a Symmetry Group

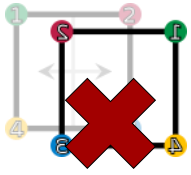

No action

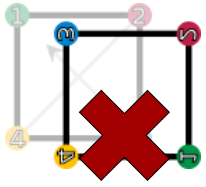

Rotation 90°

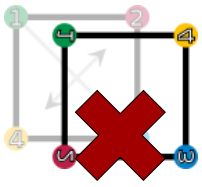

Rotation 180°


Rotation 270°


Vertical flip


Horizontal flip


Diagonal flip


Diagonal flip 2

Subgroup Conditions

- **Problem.** Let G be a group, and let H be a non-empty subset of G such that
  - **C1.** If $x, y \in H$ then $xy \in H$.
  - **C2.** If $x \in H$ then $x^{-1} \in H$.

  Prove that H is a subgroup.
  - **Closure.** By **C1**.
  - **Inverse.** By **C2**.
  - **Associativity.** By the associativity of G.
  - **Identity.** By **C2**, $x, x^{-1} \in H$. By **C1**, we have $1 = xx^{-1} \in H$.

Finite Subgroup Conditions

- **Problem.** Let G be a ***finite*** group, and let H be a non-empty subset of G such that
  - **C1.** If $x, y \in H$ then $xy \in H$.
  - ~~**C2.** If $x \in H$ then $x^{-1} \in H$.~~

  Prove that H is a subgroup.
- **Proof.** Consider $x \in H$.
- Since G is finite, the series $1, x, x^2, x^3, \ldots$ has two identical elements $x^i = x^j$ with $i < j$.
- Multiply both side by x^{-i-1} (in G) to obtain

$$x^{-1} = x^{j-i-1} = xx\cdots x \in H.$$

The End: A Noah's Ark Joke

The Flood has receded and the ark is safely aground atop Mount Ararat; Noah tells all the animals to go forth and multiply. Soon the land is teeming with every kind of living creature in abundance, except for snakes. Noah wonders why.

One morning two miserable snakes knock on the door of the ark with a complaint. "You haven't cut down any trees." Noah is puzzled, but does as they wish.

Within a month, you can't walk a step without treading on baby snakes. With difficulty, he tracks down the two parents. "What was all that with the trees?" "Ah," says one of the snakes, "you didn't notice which species we are." Noah still looks blank. "We're adders, and we can only multiply using logs."