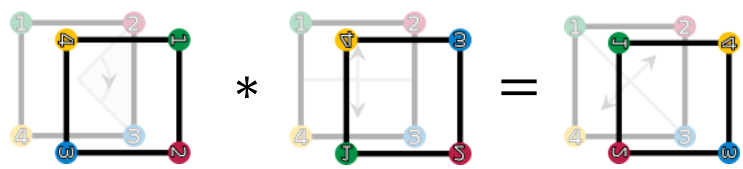
Ma/CS 6a

Class 18: Groups



Rotation 90° Vertical flip Diagonal flip 2

By Adam Sheffer

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 $x * x^{-1} = x^{-1} * x = e$.

Permutation Group

- The set S_n under the operation of composition is a group.
  - **Closure.** If $\alpha, \beta \in S_n$, then $\alpha\beta \in S_n$.
  - **Associativity.** For every $\alpha, \beta, \gamma \in S_n$, we have
    $$(\alpha\beta)\gamma = \alpha(\beta\gamma).$$
  - **Identity.** The identity permutation $\mathrm{id} \in S_n$ satisfies for every $x \in S_n$:
    $$\mathrm{id} \cdot x = x \cdot \mathrm{id} = x.$$
  - **Inverse.** For every $\alpha \in S_n$ there exists $\alpha^{-1} \in S_n$ such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \mathrm{id}$.

Is This a Group? #1

- Is the following a group? The set of integers $\mathbb{Z}$ under the addition operation.
  - **Closure.** For every two integers $x, y \in \mathbb{Z}$, $x + y$ is also in $\mathbb{Z}$.
  - **Associativity.** For every $x, y, z \in \mathbb{Z}$, we have
    $$(x + y) + z = x + (y + z).$$
  - **Identity.** The exists $0 \in \mathbb{Z}$, such that for every $x \in \mathbb{Z}$, we have
    $$0 + x = x + 0 = x.$$
  - **Inverse.** For every $x \in \mathbb{Z}$ there exists $-x \in \mathbb{Z}$ such that $x + (-x) = (-x) + x = 0$.

Is This a Group? #2

- Is the following a group? The set of integers $\mathbb{Z}$ under ***multiplication***.
  - **Closure.** For every two integers $x, y \in \mathbb{Z}$, $x \cdot y$ is also in $\mathbb{Z}$.
  - **Associativity.** For every $x, y, z \in \mathbb{Z}$, we have
    $$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$
  - **Identity.** The exists $1 \in \mathbb{Z}$, such that for every $x \in \mathbb{Z}$, we have
    $$1 \cdot x = x \cdot 1 = x.$$
  - **Inverse.** The only element that has an inverse is -1.

    Not a group!

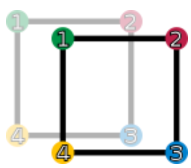
Is This a Group? #3

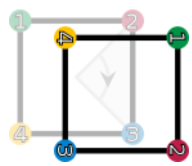
- Is the following a group? The set of integers $\mathbb{Z}$ under ***subtraction***.
  - **Closure.** For every two integers $x, y \in \mathbb{Z}$, $x - y$ is also in $\mathbb{Z}$.
  - **Associativity.** When $z \neq 0$, we have
    $$(x - y) - z \neq x - (y - z).$$
    Not a group!
  - **Identity.** The is no $e \in \mathbb{Z}$, such that for every $x \in \mathbb{Z}$, we have
    $$e - x = x - e = x.$$
    Not a group!
  - **Inverse.** Since there is no identity, there is no inverse.

    Not a group!

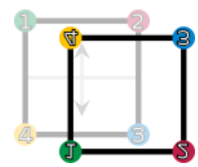
Symmetries of the Square

- S – a square.
- A *symmetry* of S is a transformation of the plane that takes S to itself and preserves distances.





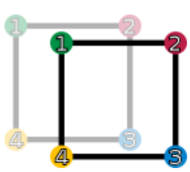
Rotation by 90°



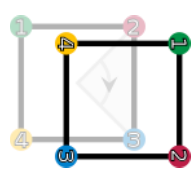
Vertical flip

Is This a Group? #4

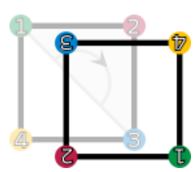
- The set of symmetries of the square is closed under composition.



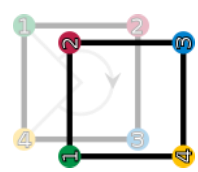
No action



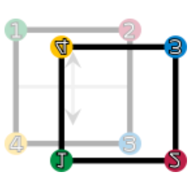
Rotation 90°



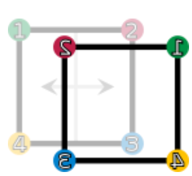
Rotation 180°



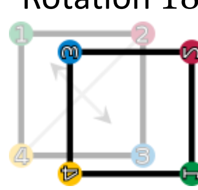
Rotation 270°



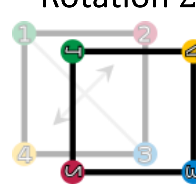
Vertical flip



Horizontal flip



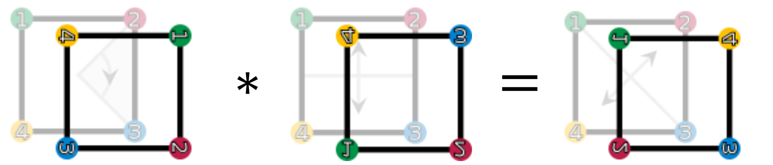
Diagonal flip



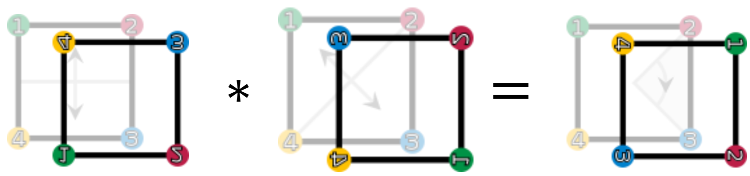
Diagonal flip 2

Symmetries have Closure

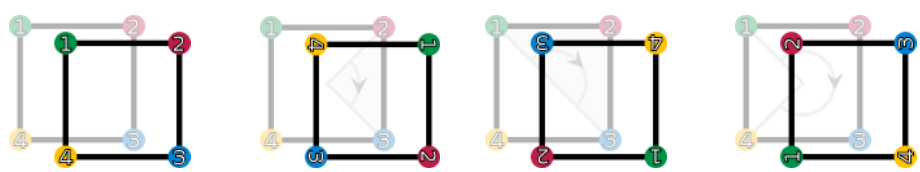
- Examples of closure (as with permutations, we first apply the second symmetry):



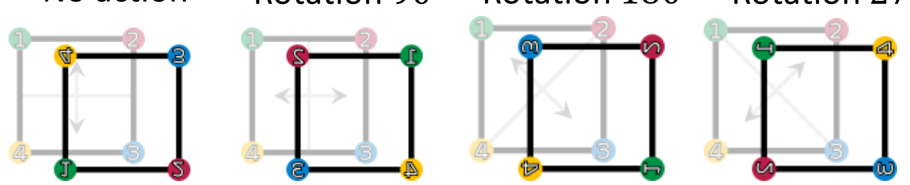
Rotation 90° * Vertical flip = Diagonal flip 2



Vertical flip * Diagonal flip = Rotation 90°



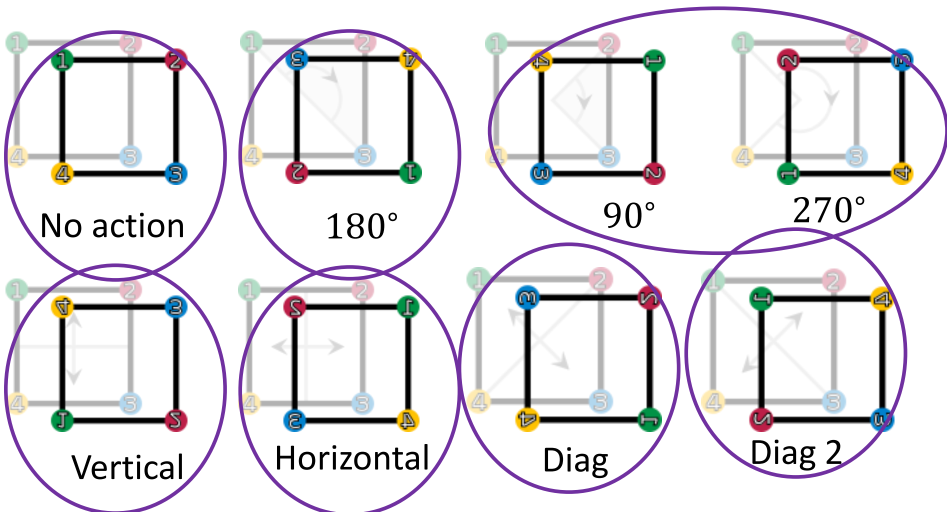
No action | Rotation 90° | Rotation 180° | Rotation 270°



Vertical flip | Horizontal flip | Diagonal flip | Diagonal flip 2

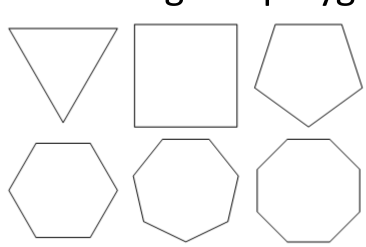
- Associativity holds.
- What is the identity element? No action.

Inverses of Symmetries



Symmetry Groups

- We obtained that the symmetries of the square form a group.
- This group is called *the symmetry group of the square*.
- We can similarly consider symmetry groups of other regular polygons.



Is This a Group? #5

- The set $\mathbb{Z}_p^+ = \{1,2,3, \dots, p-1\}$ under multiplication $mod\ p$, where p is prime.
  - **Closure.** For every $x, y \in \mathbb{Z}_p^+$, we have $(x \cdot y \bmod p) \in \mathbb{Z}_p^+$.
  - **Associativity.** Holds since standard product is associative.
  - **Identity.** The identity element is 1.
  - **Inverse.** In Lecture 2, we proved that $ax \equiv b\ mod\ p$ has a unique solution. Setting $b = 1$ implies that the inverse always exists (we also need the property $ax \equiv xa$).

Is This a Group? #6

- The set of $n \times n$ matrices of real numbers, under multiplication.
  - **Closure.** For every two matrices $A, B \in G$, AB is also an $n \times n$ matrix.
  - **Associativity.** Matrix multiplication is associative.
  - **Identity.** The identity element is a matrix with ones on the main diagonal and zero everywhere else.
  - **Inverse.** Only invertible matrices have an inverse.

Not a group!

Applications of Groups

- Groups are used ***EVERYWHERE***!
  - Algebra. Proving that there is no nice solution to equations in of degree $d \geq 5$ in one variable (in the spirit of $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$).
  - Cryptography. Elliptic curve cryptography.
  - Chemistry. Studying what types of crystal structures can exist.
  - Fourier analysis, error correcting codes, combinatorics,…

Évariste Galois

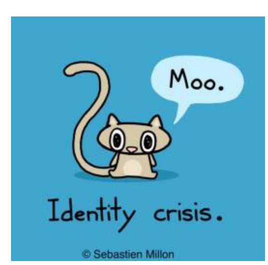
- French mathematician (1811-1832).
- Died in a duel at the age of 20.
- By then, managed to lay the foundations of group theory (and a couple of other major contributions).

Is This a Group? #7

- 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.
- **Closure.** The product of matrices of G:
$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha\gamma & \alpha\delta + \beta \\ 0 & 1 \end{pmatrix}.$$
- **Associativity.** Matrix multiplication is associative.

Is This a Group? #7

- 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.
  - **Identity.** We have
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$$



Is This a Group? #7

- 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.
  - **Inverse.** We need to solve
$$\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \gamma & \delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
That is, $\alpha\gamma = 1$ and $\alpha\delta + \beta = 0$. This system always has a solution mod 3.

Change of Notation

- For simplicity, we replace the $*$ notation with standard multiplication notation.
  - Replace $x * y$ with xy.
  - The identity element is 1.
  - The inverse of x is x^{-1}.

Cancellation Laws

- **Claim.** Let G be a group and let $x, y, z \in G$.

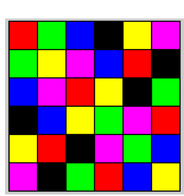
$$xy = xz \quad \rightarrow \quad y = z,$$
$$yx = zx \quad \rightarrow \quad y = z.$$

- **Proof.** Multiply both side by x^{-1}:

$$x^{-1}(xy) = x^{-1}(xz)$$
$$(x^{-1}x)y = (x^{-1}x)z$$
$$y = z$$

Latin Squares

- Consider a group G with element set
$$\{g_1, g_2, \dots, g_n\}.$$
- g_i – an arbitrary element of G.
- By the cancellation law, each of the products $g_i g_1, g_i g_2, \dots, g_i g_n$ are distinct.
- Similarly for $g_1 g_i, g_2 g_i \dots g_n g_i$.
- The multiplication table is a *Latin square*!



A	B	C	D	E
B	C	D	E	A
C	D	E	A	B
D	E	A	B	C
E	A	B	C	D

Unique Solution

- **Claim.** For any group G and elements $a, b \in G$, the following equation has a *unique solution*:
$$ax = b.$$
- The element $a^{-1}b$ is a solution, so there is at least one solution.
- Assume, for contradiction, that there are two solutions x, x'. We have $ax = ax'$, so by the cancellation law $x = x'$.
- Thus, there is a unique solution.

Corollaries

- **Claim.** The *identity element* of a group is *unique*.
- **Proof.** For any $a \in G$, there is a unique solution to $ax = a$.
- **Claim.** Every element of G has a *unique inverse*.
- **Proof.** For any $a \in G$, there is a unique solution to $ax = 1$.

Recap: Group Properties

- **Closure.** For every $x, y \in G$, we have $xy \in G$.
- **Associativity.** For every $x, y, z \in G$, we have
$$(xy)z = x(yz).$$
- **Identity.** There exists a unique $1 \in G$, such that for every $x \in G$, we have
$$1x = x1 = x.$$
- **Inverse.** For every $x \in G$ there exists a unique inverse $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = 1$.
- **Latin table.** The multiplication table of G is a Latin table.

The Order of a Group

- The ***order of a group*** is the number of elements in its set.
  - The group of symmetries of the square is of order 8.
  - The group of matrices of the form $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$ where $\alpha \in \{1,2\}$ and $\beta \in \{0,1,2\}$ is of order 6.
  - The group of integers under addition is of ***infinite order***.

Powers

- Consider a group G and an element $a \in G$. For $k \in \mathbb{N}$, we write

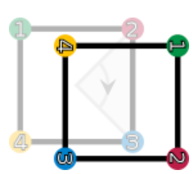
$$a^k = aaa \cdots a,$$
$$a^{-k} = a^{-1}a^{-1} \cdots a^{-1},$$
$$a^0 = 1.$$

- As with standard multiplication, we have

$$a^{m+n} = a^m a^n,$$
$$a^{mn} = (a^m)^n.$$

The Order of an Element

- a – an element of the group G.
- The *order of an element* a is the least positive integer k that satisfies $a^k = 1$.
- What is the order of



Rotation $90°$

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

(under multiplication mod 3)

$\boxed{5}$

(under integer addition)

4 2 ∞

Powers that Equal to 1

- **Claim.** Let a be an element of order m in a finite group. Then $a^s = 1$ iff $m|s$.
- **Proof.**
  - Assume $m|s$. then there exists k such that $s = mk$. Thus $a^s = a^{mk} = (a^m)^k = 1^k = 1$.
  - Assume $a^s = 1$. There exist integers q and $0 \leq r < m$ such that $s = mq + r$, so
    $$1 = a^s = a^{mq+r} = (a^m)^q a^r = a^r.$$
    If $r \neq 0$, this contradicts the order of a being m. Thus, $r = 0$ and $m|s$.

More About Group Identities