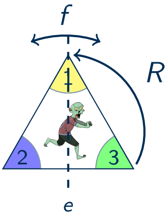
Groups and Subgroups

Dr. Chuck Rocca

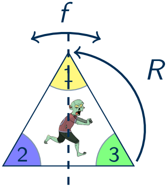
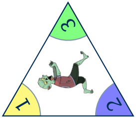
WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

Table of Contents

Triangular Symmetries

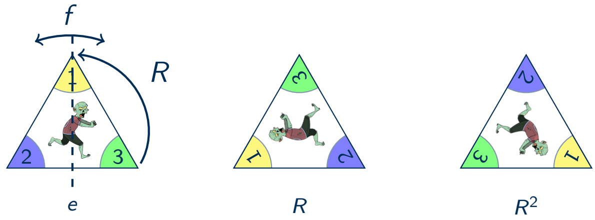
	e	R	R^2
e			
f			

Triangular Symmetries

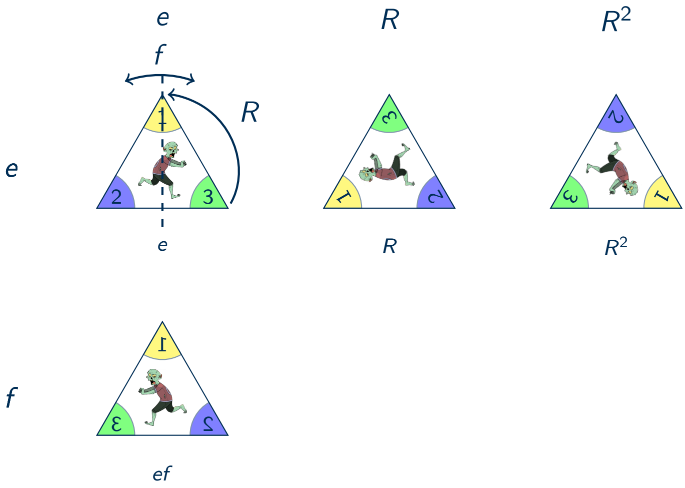
	e	R	R^2
e	 e	 R	
f			

Triangular Symmetries

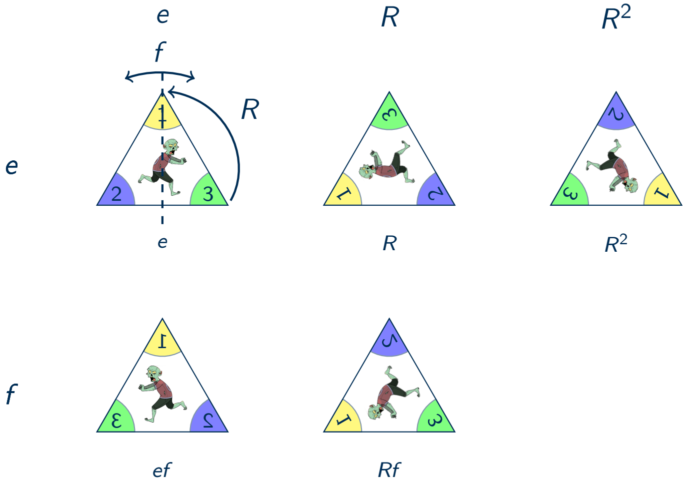
	e	R	R^2
e			
f			



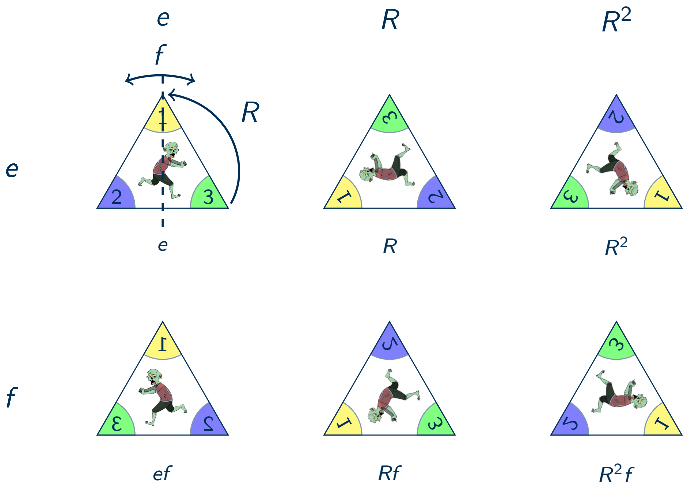
Triangular Symmetries



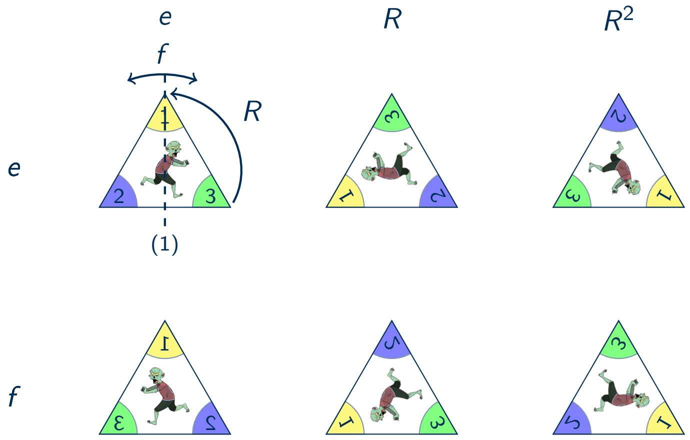
Triangular Symmetries



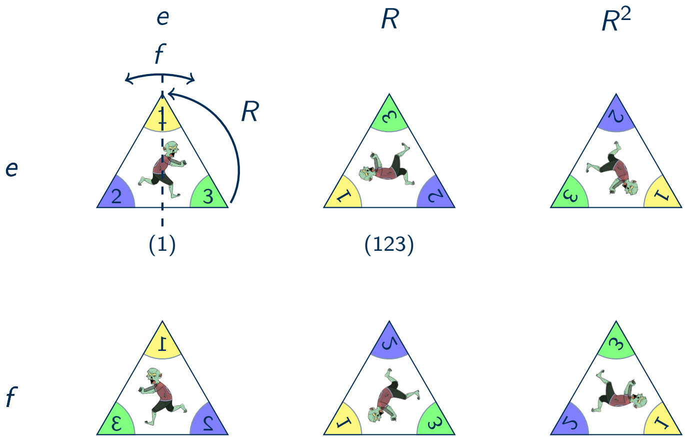
Triangular Symmetries



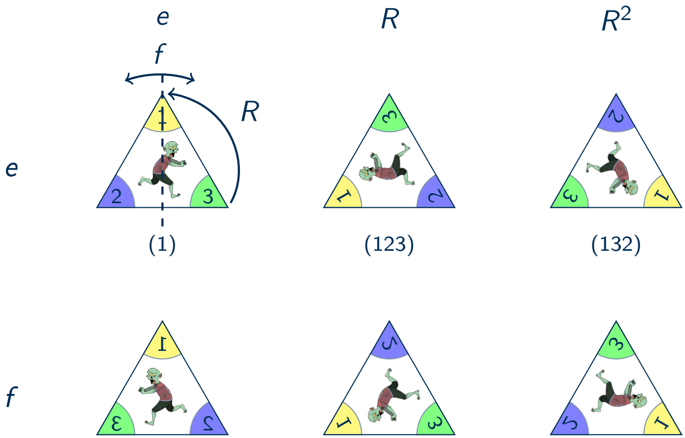
Focus on Permutations



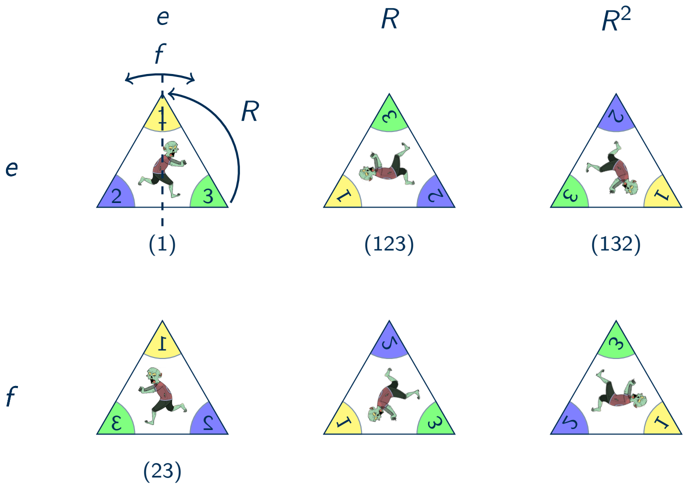
Focus on Permutations



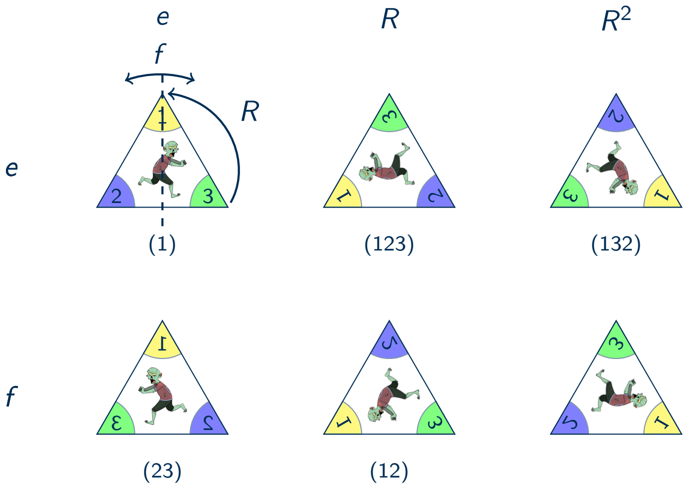
Focus on Permutations



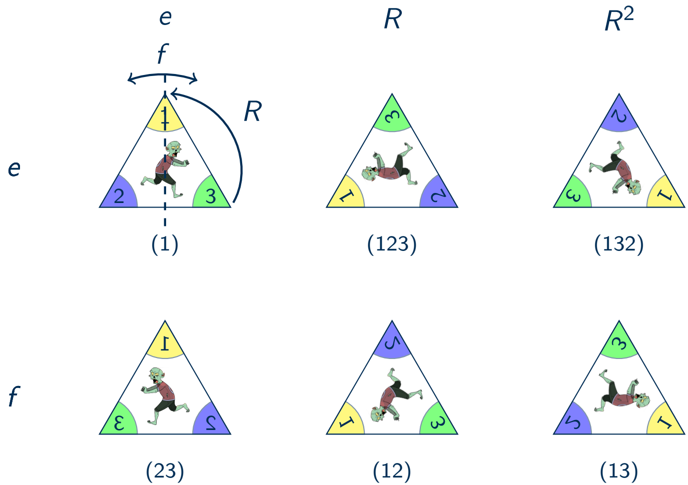
Focus on Permutations



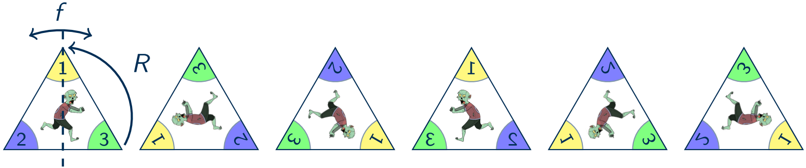
Focus on Permutations



Focus on Permutations

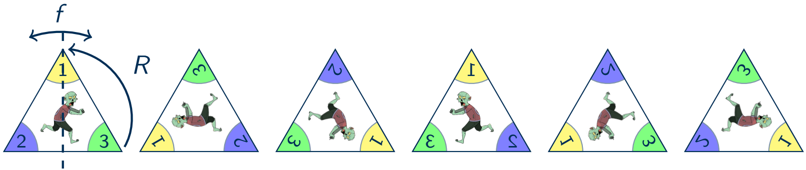


Permutations vs. Symmetries



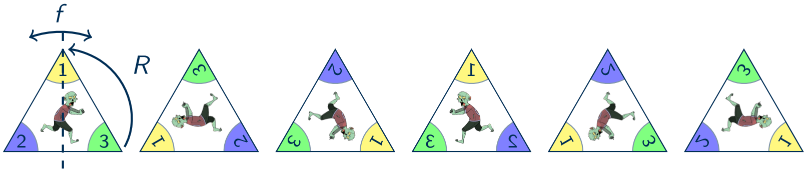
- $e = (1)$

Permutations vs. Symmetries



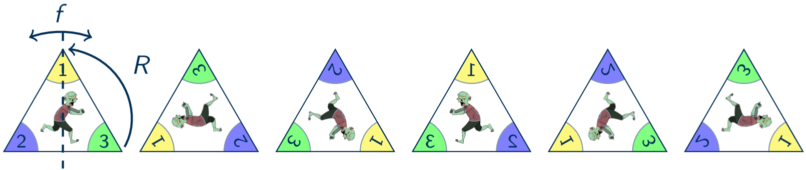
- $e = (1)$
- $R = (123)$

Permutations vs. Symmetries



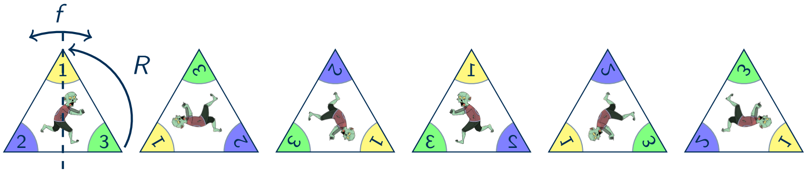
- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$

Permutations vs. Symmetries



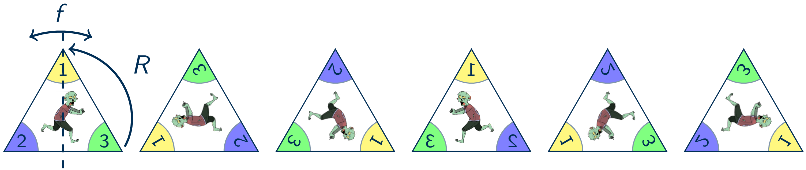
- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$
- $f = (23)$

Permutations vs. Symmetries



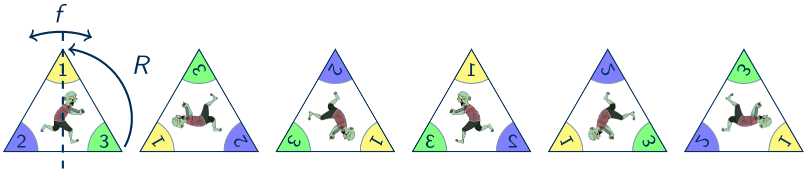
- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$
- $f = (23)$
- $Rf = (12) = (123)(23)$

Permutations vs. Symmetries



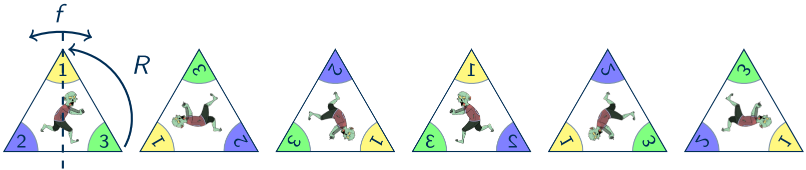
- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$
- $f = (23)$
- $Rf = (12) = (123)(23)$
- $R^2 f = (13) = (132)(23)$

Permutations vs. Symmetries



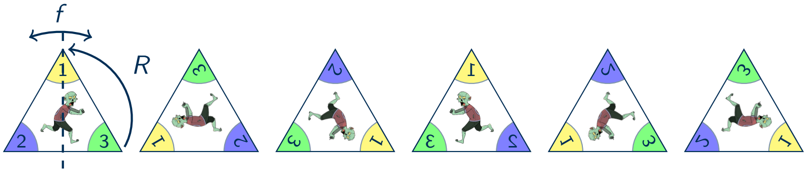
- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$
- $f = (23)$
- $Rf = (12) = (123)(23)$
- $R^2 f = (13) = (132)(23)$
- $fR = (23)(123) = (13)$

Permutations vs. Symmetries



- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$
- $f = (23)$
- $Rf = (12) = (123)(23)$
- $R^2f = (13) = (132)(23)$
- $fR = (23)(123) = (13)$
- $fR^2 = (23)(132) = (12)$

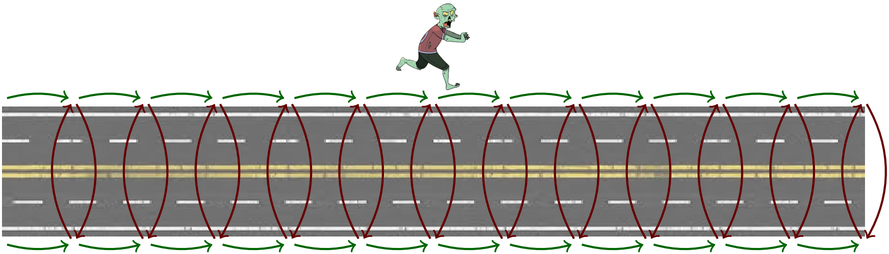
Permutations vs. Symmetries



- $e = (1)$
- $R = (123)$
- $R^2 = (132) = (123)(123)$
- $f = (23)$
- $Rf = (12) = (123)(23)$
- $R^2f = (13) = (132)(23)$
- $fR = (23)(123) = (13)$
- $fR^2 = (23)(132) = (12)$

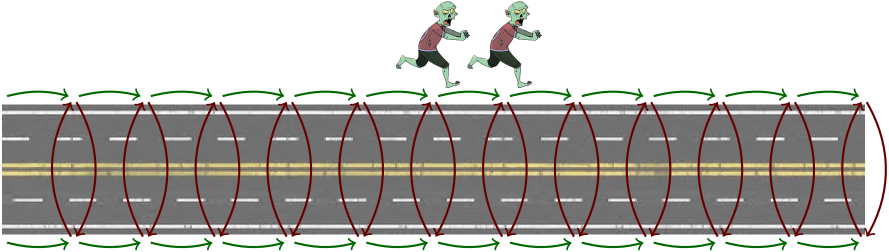
$$fr^k = r^{3-k}f$$

Shifts and Flips



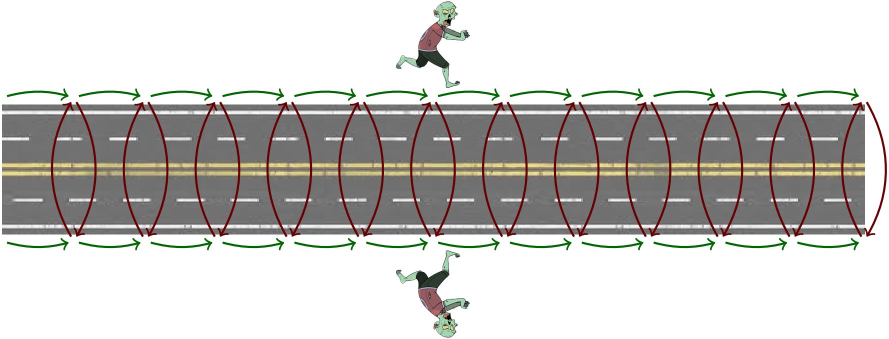
Shifts and Flips

$$(Shift, Flip) = (1, 0) = (1, 2n)$$



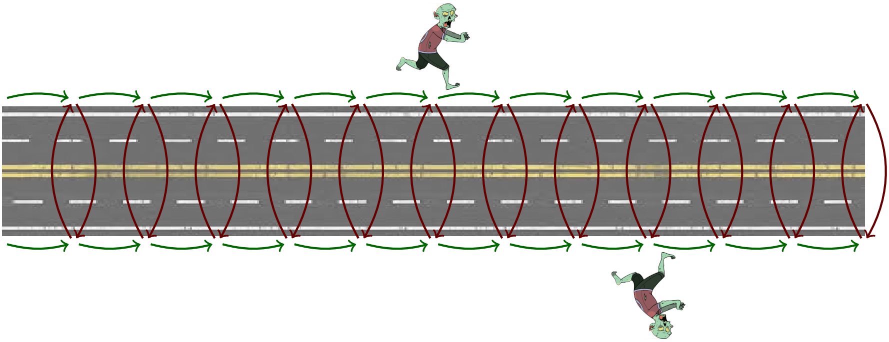
Shifts and Flips

$$(Shift, Flip) = (0, 1) = (0, 2n + 1)$$



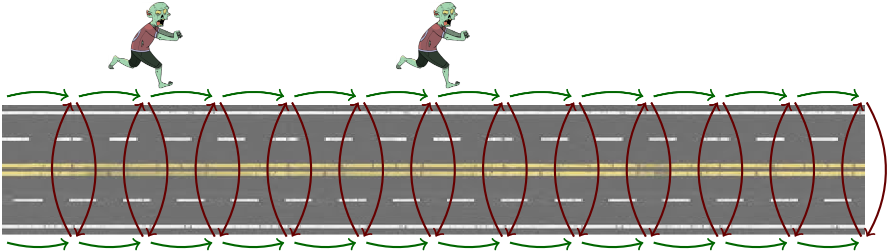
Shifts and Flips

$$(Shift, Flip) = (3, 1) = (3, 2n + 1)$$



Shifts and Flips

$$(Shift, Flip) = (-4, 0) = (-4, 2n)$$



Direct Product: $\mathbb{Z} \oplus \mathbb{Z}_2$

$$\mathbb{Z} \oplus \mathbb{Z}_2 = \{(a, b) | a \in \mathbb{Z},\ b \in \mathbb{Z}_2\}$$

and

$$\forall (a, b), (c, d) \in \mathbb{Z} \oplus \mathbb{Z}_2 : (a, b) + (c, d) = (a + c, b + d)$$

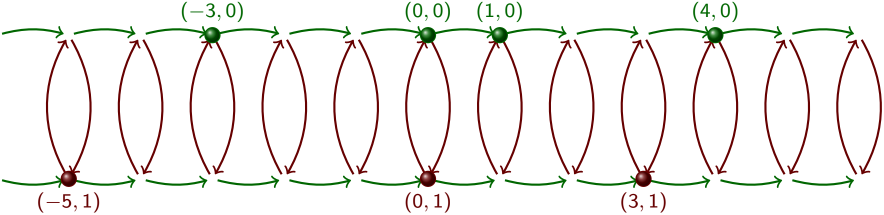


Table of Contents

Group Definition

Definition (Group)

A **group** is a set G together with a binary operation $*$ such that

1. Closure: $\forall a, b \in G : a * b \in G$
2. Associative: $\forall a, b, c \in G : a * (b * c) = (a * b) * c$
3. Identity: $\exists e \in G \ \forall a \in G : e * a = a * e = a$
4. Inverses: $\forall a \in G \ \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$

Dihedral Group: $(D_n, \circ)$

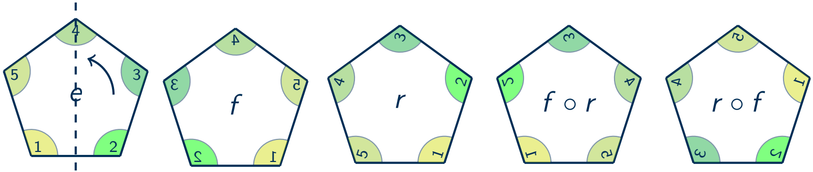
Definition

The **Dihedral Group,** D_n is the set of all transformations of an n-gon which leave it fixed as a set, i.e. it appears the same, they are combined using composition. It can be **generated** by a single reflection, f, perpendicular to a side and a rotation of $r = 360^\circ/n$. The **order of** D_n is $|D_n| = 2n$ and it is **non-Abelian**.

Dihedral Group: $(D_n, \circ)$

Definition

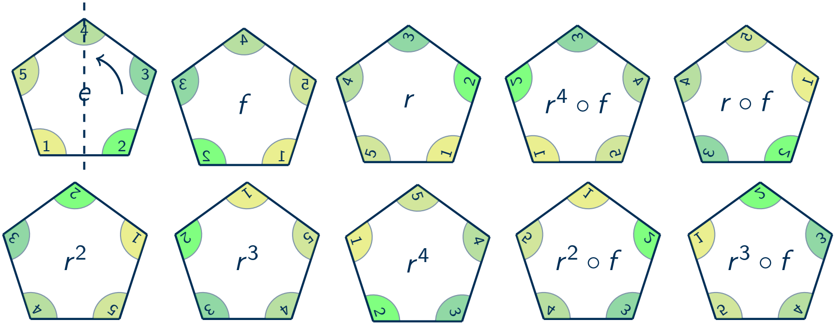
The **Dihedral Group,** D_n is the set of all transformations of an n-gon which leave it fixed as a set, i.e. it appears the same, they are combined using composition. It can be **generated** by a single reflection, f, perpendicular to a side and a rotation of $r = 360^\circ/n$. The **order of** D_n is $|D_n| = 2n$ and it is **non-Abelian**.



Dihedral Group: $(D_n, \circ)$

Definition

The **Dihedral Group,** D_n is the set of all transformations of an n-gon which leave it fixed as a set, i.e. it appears the same, they are combined using composition. It can be **generated** by a single reflection, f, perpendicular to a side and a rotation of $r = 360^\circ/n$. The **order of** D_n is $|D_n| = 2n$ and it is **non-Abelian**.



Orders

Definition

If G is a group, the **order of** G is the number of elements in G and is written $|G|$.

Orders

Definition

If G is a group, the **order of** G is the number of elements in G and is written $|G|$.

Definition

If G is a group and $g \in G$, then **the order of** g is the **least** positive integer k such that $g^k = e \in G$ and is written $|g| = k$. If no such value exists we say $|g| = \infty$.

A Theorem on Orders

Theorem

Given $g \in G$, a group, assume $|g| = k$:

1. *if $g^l = e$, then $k|l$,*
2. *if $g^i = g^j$, then $i \equiv j \pmod{k}$, and*
3. *if $k = qd$, then $|g^d| = q$.*

A Theorem on Orders

Part 1.

□

A Theorem on Orders

Part 1.

1. Assume $|g| = k$ and $g^l = e$

□

A Theorem on Orders

Part 1.

1. Assume $|g| = k$ and $g^l = e$
2. $l = qk + r$ with $0 \leq r < k$

□

A Theorem on Orders

Part 1.

1. Assume $|g| = k$ and $g^l = e$
2. $l = qk + r$ with $0 \leq r < k$
3. $e = g^l = g^{qk+r} = (g^k)^q g^r = eg^r = g^r$

□

A Theorem on Orders

Part 1.

1. Assume $|g| = k$ and $g^l = e$
2. $l = qk + r$ with $0 \leq r < k$
3. $e = g^l = g^{qk+r} = (g^k)^q g^r = eg^r = g^r$
4. $r = 0$ or we contradict the assumption that k is least

$\square$

A Theorem on Orders

Part 1.

1. Assume $|g| = k$ and $g^l = e$
2. $l = qk + r$ with $0 \leq r < k$
3. $e = g^l = g^{qk+r} = (g^k)^q g^r = eg^r = g^r$
4. $r = 0$ or we contradict the assumption that k is least
5. $\therefore k | l$

$\square$

A Theorem on Orders

Theorem

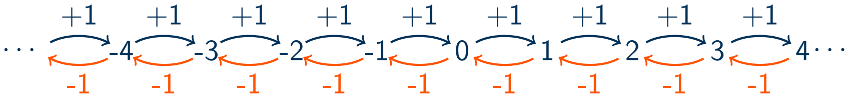
Given $g \in G$, a group, assume $|g| = k$:

1. *if $g^l = e$, then $k|l$,*
2. *if $g^i = g^j$, then $i \equiv j \pmod{k}$, and*
3. *if $k = qd$, then $|g^d| = q$.*

Integers: $(\mathbb{Z}, +)$

Integers: $(\mathbb{Z}, +)$

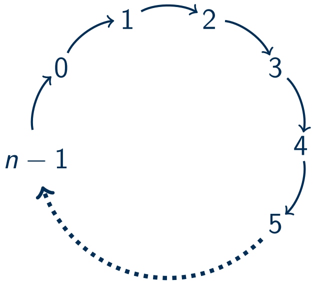
The **integers,** $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ form a group with addition. Since for all $a, b \in \mathbb{Z}$ $a + b = b + a$, we say that $\mathbb{Z}$ is an **Abelian** group. The order of $\mathbb{Z}$ is infinite, $|\mathbb{Z}| = \infty$. Finally, since we get all the elements of $\mathbb{Z}$ by adding and subtracting 1, we say $\mathbb{Z}$ is a **cyclic group**.



Integers Modulo n: $(\mathbb{Z}_n, +)$

Integers: $(\mathbb{Z}_n, +)$

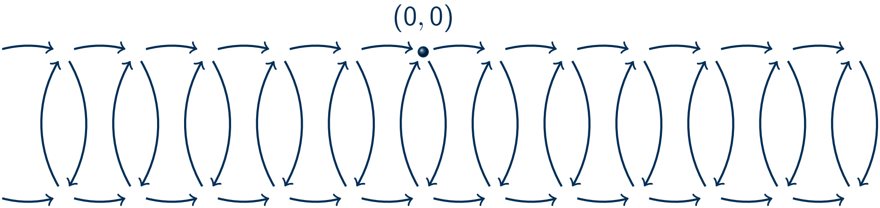
The **integers modulo** n**,** $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ form a group with addition. Since for all $a, b \in \mathbb{Z}_n$ $a + b = b + a$, we say that $\mathbb{Z}_n$ is an **Abelian** group. The order of $\mathbb{Z}_n$ is n, $|\mathbb{Z}| = n$. Finally, since we get all the elements of $\mathbb{Z}_n$ by adding 1, we say $\mathbb{Z}_n$ is a **cyclic group**.



Direct Product: $(\mathbb{Z} \oplus \mathbb{Z}_n, +)$

Integers: $(\mathbb{Z} \oplus \mathbb{Z}_n, +)$

The set $\mathbb{Z} \oplus \mathbb{Z}_n = \{(a, b) | a \in \mathbb{Z},\ b \in \mathbb{Z}_n\}$ is a group using addition where $(a, b) + (c, d) = (a + c, b + d)$. Since each component is Abelian, this group is Abelian, its order is infinite, but it has a finite **subgroup**. (This is called the **torsion subgroup**.)



Direct Product: $(G_1 \oplus G_2, *)$

Definition

Given two groups G_1 and G_2 a **direct product** of the groups is the set

$$G_1 \oplus G_2 = \{(a, b) | a \in G_1, b \in G_2\}$$

with the operation

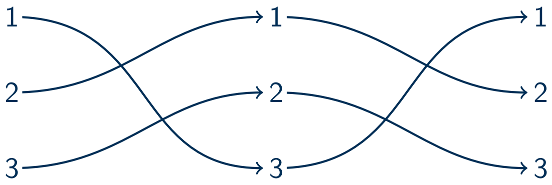
$$(a, b) * (c, d) = (a *_{G_1} c, b *_{G_2} d).$$

The order of $|G_1 \oplus G_2| = |G_1||G_2|$ if they are finite, otherwise it is infinite.

Symmetric Group: $(S_n, \circ)$

Definition

The **symmetric group $\mathbf{S_n}$** is the set of all permutations of n objects. Permutations are combined using composition and since there are $n!$ ways to permute n objects, the order of S_n is $|S_n| = n!$

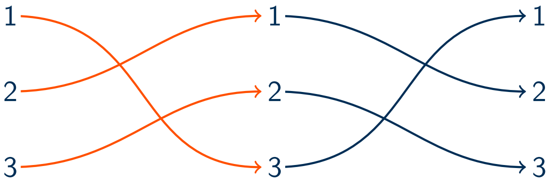


$$(123) \circ (132) = (1)$$

Symmetric Group: $(S_n, \circ)$

Definition

The **symmetric group $\mathbf{S_n}$** is the set of all permutations of n objects. Permutations are combined using composition and since there are $n!$ ways to permute n objects, the order of S_n is $|S_n| = n!$

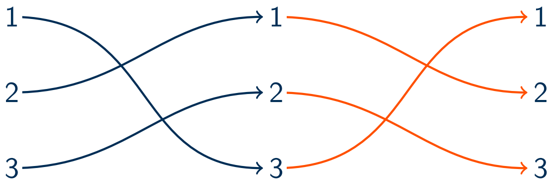


$$(123) \circ (132) = (1)$$

Symmetric Group: $(S_n, \circ)$

Definition

The **symmetric group $\mathbf{S_n}$** is the set of all permutations of n objects. Permutations are combined using composition and since there are $n!$ ways to permute n objects, the order of S_n is $|S_n| = n!$

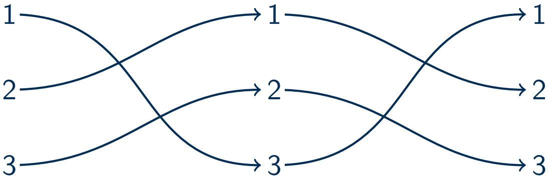


$$(123) \circ (132) = (1)$$

Symmetric Group: $(S_n, \circ)$

Definition

The **symmetric group $\mathbf{S_n}$** is the set of all permutations of n objects. Permutations are combined using composition and since there are $n!$ ways to permute n objects, the order of S_n is $|S_n| = n!$



$$(123) \circ (132) = (1)$$

A Couple Observations

Trivial Group

The set containing only the identity $G = \{e\}$ is a group and is called the **trivial group**.

A Couple Observations

Trivial Group

The set containing only the identity $G = \{e\}$ is a group and is called the **trivial group**.

Rings and Groups

Every ring is an Abelian group using its "addition" operation. Also, the non-zero elements of every field, or units in a ring, form a group using its "multiplication."

Some General Properties

Theorem

Let G be a group and let $a, b, c \in G$, then we have the following properties:

1. *G has a unique identity element,*
2. *Every element in G has a unique inverse,*
3. *Right and left cancellation hold:*
   - $ab = ac$ *implies* $b = c$
   - $ba = ca$ *implies* $b = c$
4. $(ab)^{-1} = b^{-1}a^{-1}$
5. $(a^{-1})^{-1} = a$

Table of Contents

Subgroups

Definition

If G is a group and H is a subset of G which is also a group using the same operation as G, then we say that H is a **subgroup** of G.

Dihedral Subgroups

If $G = D_6$, then the following are subgroups of G:

- $H = \langle r \rangle = \{r, r^2, r^3, \ldots, r^5, e\} \cong \mathbb{Z}_6$, this is the **cyclic subgroup generated by** r

Dihedral Subgroups

If $G = D_6$, then the following are subgroups of G:

- $H = \langle r \rangle = \left\{r, r^2, r^3, \ldots, r^5, e\right\} \cong \mathbb{Z}_6$, this is the **cyclic subgroup generated by** r
- $K = \langle f \rangle = \{f, e\} \cong \mathbb{Z}_2$, this is the cyclic subgroup generated by f

Dihedral Subgroups

If $G = D_6$, then the following are subgroups of G:

- $H = \langle r \rangle = \{r, r^2, r^3, \ldots, r^5, e\} \cong \mathbb{Z}_6$, this is the **cyclic subgroup generated by** r
- $K = \langle f \rangle = \{f, e\} \cong \mathbb{Z}_2$, this is the cyclic subgroup generated by f
- $J = \langle r^2 \rangle = \{r^2, r^4, e\} \cong \mathbb{Z}_3$, this is the cyclic subgroup generated by r^2

Dihedral Subgroups

If $G = D_6$, then the following are subgroups of G:

- $H = \langle r \rangle = \left\{ r, r^2, r^3, \ldots, r^5, e \right\} \cong \mathbb{Z}_6$, this is the **cyclic subgroup generated by** r
- $K = \langle f \rangle = \{ f, e \} \cong \mathbb{Z}_2$, this is the cyclic subgroup generated by f
- $J = \left\langle r^2 \right\rangle = \left\{ r^2, r^4, e \right\} \cong \mathbb{Z}_3$, this is the cyclic subgroup generated by r^2
- $M = \left\langle r^2, f \right\rangle = \left\{ r^2, r^4, e, r^2 f, r^4 f, f \right\} \cong D_3$

Dihedral Subgroups

If $G = D_6$, then the following are subgroups of G:

- $H = \langle r \rangle = \left\{ r, r^2, r^3, \ldots, r^5, e \right\} \cong \mathbb{Z}_6$, this is the **cyclic subgroup generated by** r
- $K = \langle f \rangle = \{ f, e \} \cong \mathbb{Z}_2$, this is the cyclic subgroup generated by f
- $J = \left\langle r^2 \right\rangle = \left\{ r^2, r^4, e \right\} \cong \mathbb{Z}_3$, this is the cyclic subgroup generated by r^2
- $M = \left\langle r^2, f \right\rangle = \left\{ r^2, r^4, e, r^2 f, r^4 f, f \right\} \cong D_3$
- Trivial Subgroup $\langle e \rangle$

Dihedral Subgroups

If $G = D_6$, then the following are subgroups of G:

- $H = \langle r \rangle = \{r, r^2, r^3, \ldots, r^5, e\} \cong \mathbb{Z}_6$, this is the **cyclic subgroup generated by** r
- $K = \langle f \rangle = \{f, e\} \cong \mathbb{Z}_2$, this is the cyclic subgroup generated by f
- $J = \langle r^2 \rangle = \{r^2, r^4, e\} \cong \mathbb{Z}_3$, this is the cyclic subgroup generated by r^2
- $M = \langle r^2, f \rangle = \{r^2, r^4, e, r^2 f, r^4 f, f\} \cong D_3$
- Trivial Subgroup $\langle e \rangle$
- Entire Group $G = D_6$

Dihedral Subgroups

If $G = D_n$, then the following are subgroups of G:

- $H = \langle r \rangle = \{r, r^2, r^3, \ldots, r^{n-1}, e\} \cong \mathbb{Z}_n$, this is the **cyclic subgroup generated by** r
- $K = \langle f \rangle = \{f, e\} \cong \mathbb{Z}_2$, this is the cyclic subgroup generated by f
- $J = \langle r^j \rangle = \{r^j, r^{2j}, \ldots, r^{(q-1)j}, e\} \cong \mathbb{Z}_q$ for $n = qj$, this is the cyclic subgroup generated by r^j
- $M = \langle r^j, f \rangle = \{r^j, \ldots, r^{(q-1)j}, e, r^j f, \ldots, r^{(q-1)j} f, f\} \cong D_q$ for $n = qj$
- Trivial Subgroup $\langle e \rangle$
- Entire Group $G = D_n$

Subgroups Generated by Elements

Definition

If G is a group and $g \in G$, then the **cyclic subgroup generated by** g is

$$\langle g \rangle = \left\{ g^i \middle| i \in \mathbb{Z} \right\}$$

which is **isomorphic** to $\mathbb{Z}$ if $|g| = \infty$ or $\mathbb{Z}_n$ if $|g| = n$,

Subgroups Generated by Elements

Definition

If G is a group and $g \in G$, then the **cyclic subgroup generated by** g is

$$\langle g \rangle = \left\{ g^i \middle| i \in \mathbb{Z} \right\}$$

which is **isomorphic** to $\mathbb{Z}$ if $|g| = \infty$ or $\mathbb{Z}_n$ if $|g| = n$,

Definition

If G is a group and $K \subset G$, then the **subgroup generated by** K, $\langle K \rangle$, is defined to be the smallest subgroup of G containing all the elements of K.

Subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$

- If $G = \mathbb{Z}$, then for all $n \in \mathbb{Z}$

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$$

  is a subgroup of G.

Subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$

- If $G = \mathbb{Z}$, then for all $n \in \mathbb{Z}$

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$$

  is a subgroup of G.

- If $G = \mathbb{Z}_n$ and $n = qj$, then

$$H = \{0, j, 2j, 3j, \ldots (q-1)j\}$$

  is a subgroup of G.

A Non-Subgroup

- The set of all units modulo 10, $U_{10} = \{1, 3, 7, 9\}$, is a group using **multiplication**. But, this is not a subgroup of $\mathbb{Z}_{10}$ because the operation in $\mathbb{Z}_{10}$ is **addition**.

A Non-Subgroup

- The set of all units modulo 10, $U_{10} = \{1, 3, 7, 9\}$, is a group using **multiplication**. But, this is not a subgroup of $\mathbb{Z}_{10}$ because the operation in $\mathbb{Z}_{10}$ is **addition**.
- Or, in general, the set of all units modulo n,

$$U_n = \{k | k \in \mathbb{Z}_n \wedge (k, n) = 1\}$$

, is a group using **multiplication**. But, it is not a subgroup of $\mathbb{Z}_n$ because the operation in $\mathbb{Z}_n$ is **addition**.

A Non-Subgroup

- The set of all units modulo 10, $U_{10} = \{1, 3, 7, 9\}$, is a group using **multiplication**. But, this is not a subgroup of $\mathbb{Z}_{10}$ because the operation in $\mathbb{Z}_{10}$ is **addition**.
- Or, in general, the set of all units modulo n,

  $$U_n = \{k | k \in \mathbb{Z}_n \wedge (k, n) = 1\}$$

  , is a group using **multiplication**. But, it is not a subgroup of $\mathbb{Z}_n$ because the operation in $\mathbb{Z}_n$ is **addition**.
- The set of real numbers, $\mathbb{R}$, is a group with addition and non-zero reals, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group with multiplication. The latter is not a subgroup of the former.

A Non-Subgroup

- The set of all units modulo 10, $U_{10} = \{1, 3, 7, 9\}$, is a group using **multiplication**. But, this is not a subgroup of $\mathbb{Z}_{10}$ because the operation in $\mathbb{Z}_{10}$ is **addition**.
- Or, in general, the set of all units modulo n,

  $$U_n = \{k | k \in \mathbb{Z}_n \land (k, n) = 1\}$$

  , is a group using **multiplication**. But, it is not a subgroup of $\mathbb{Z}_n$ because the operation in $\mathbb{Z}_n$ is **addition**.
- The set of real numbers, $\mathbb{R}$, is a group with addition and non-zero reals, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group with multiplication. The latter is not a subgroup of the former.
- In general every ring R is an Abelian group using "addition" and the subset of units of R is a group with the "multiplication." But, the subset is not a subgroup.

Subgroup Tests

Theorem (Two-Step Subgroup Test)

A non-empty subset H of a group G is subgroup of G if

1. *H is closed: $\forall a, b \in H : ab \in H$*
2. *Inverses are in H: $\forall a \in H : a^{-1} \in H$*

Subgroup Tests

Theorem (Two-Step Subgroup Test)

A non-empty subset H of a group G is subgroup of G if

1. *H is closed:* $\forall a, b \in H : ab \in H$
2. *Inverses are in H:* $\forall a \in H : a^{-1} \in H$

Proof.

1. Associativity is "inherited,"

□

Subgroup Tests

Theorem (Two-Step Subgroup Test)

A non-empty subset H of a group G is subgroup of G if

1. *H is closed: $\forall a, b \in H : ab \in H$*
2. *Inverses are in H: $\forall a \in H : a^{-1} \in H$*

Proof.

1. Associativity is "inherited,"
2. Closure and inverses are given, and

□

Note that if G is finite, then condition (1) implies condition (2).

Subgroup Tests

Theorem (Two-Step Subgroup Test)

A non-empty subset H of a group G is subgroup of G if

1. *H is closed:* $\forall a, b \in H : ab \in H$
2. *Inverses are in H:* $\forall a \in H : a^{-1} \in H$

Proof.

1. Associativity is "inherited,"
2. Closure and inverses are given, and
3. $a \in H$ implies $a^{-1} \in H$, so $aa^{-1} = e \in H$

□

Note that if G is finite, then condition (1) implies condition (2).

Example Subgroup Test

Prove n$\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

1. Let $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{qn | q \in \mathbb{Z}\}$

Example Subgroup Test

Prove n$\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

1. Let $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{qn | q \in \mathbb{Z}\}$
2. $a \in H$ implies $a = q_a n$ and $-a = -q_a n$; $-a \in H$

Example Subgroup Test

Prove n$\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

1. Let $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{qn | q \in \mathbb{Z}\}$
2. $a \in H$ implies $a = q_a n$ and $-a = -q_a n$; $-a \in H$
3. $a = q_a n$ and $b = q_b n$ in H implies

$$a + b = q_a n + q_b n = (q_a + q_b)n$$

   is also in H

Example Subgroup Test

Prove n$\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

1. Let $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{qn | q \in \mathbb{Z}\}$
2. $a \in H$ implies $a = q_a n$ and $-a = -q_a n$; $-a \in H$
3. $a = q_a n$ and $b = q_b n$ in H implies

$$a + b = q_a n + q_b n = (q_a + q_b)n$$

   is also in H

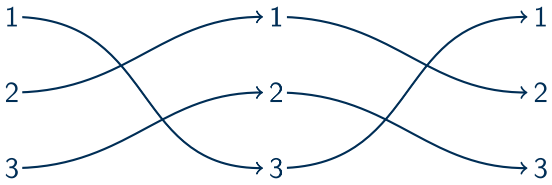
4. $\therefore$ by the 2-Step Subgroup Test $H = n\mathbb{Z}$ is a subgroup of $G = \mathbb{Z}$

Table of Contents

Symmetric Group: $(S_n, \circ)$

Definition

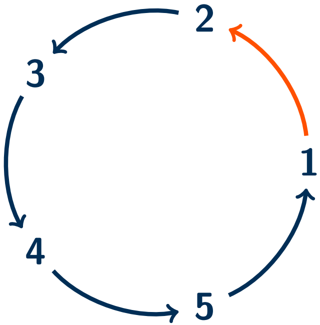
The **symmetric group $\mathbf{S_n}$** is the set of all permutations of n objects. Permutations are combined using composition and since there are $n!$ ways to permute n objects, the order of S_n is $|S_n| = n!$



$$(123) \circ (132) = (1)$$

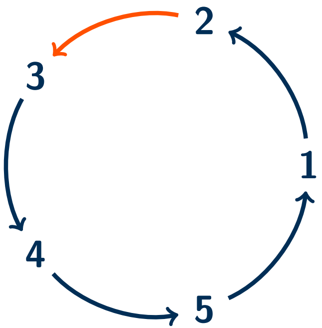
Cycle Notation Concept

$$(12345)$$



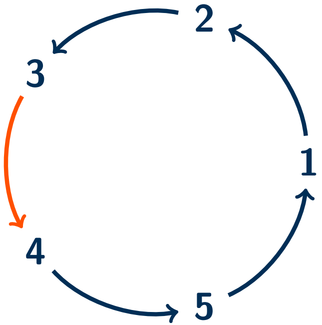
Cycle Notation Concept

$$(12345)$$



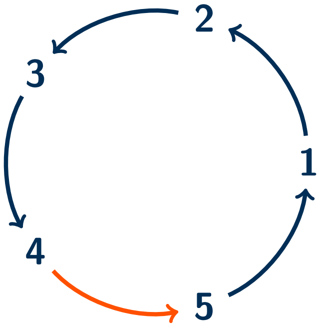
Cycle Notation Concept

$$(12345)$$



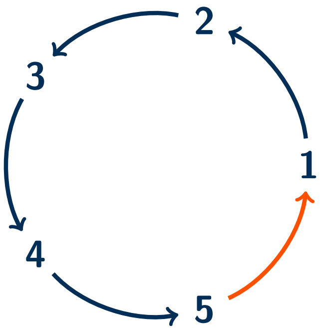
Cycle Notation Concept

$$(12345)$$

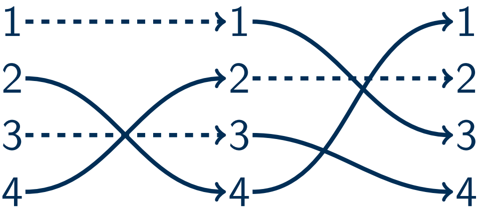


Cycle Notation Concept

$$(12345)$$

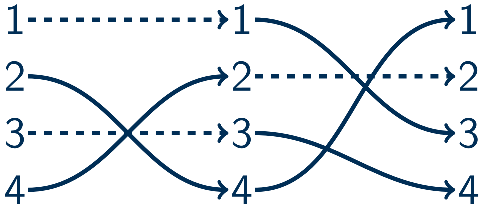


Cycle Notation Composition



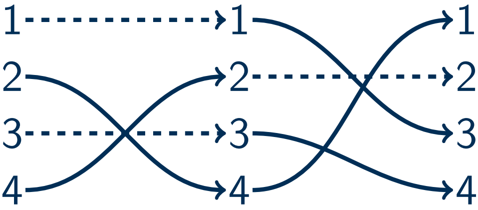
$$(134)(24) = (1342)$$

Cycle Notation Composition



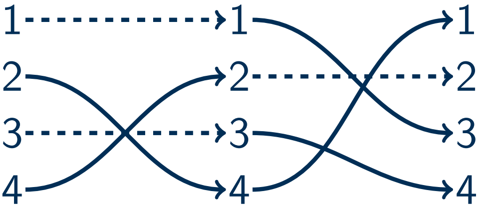
$$(134)(24) = (1342)$$

Cycle Notation Composition



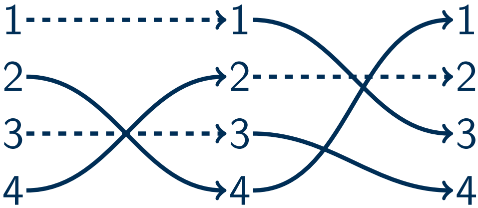
$$(134)(24) = (1342)$$

Cycle Notation Composition



$$(134)(24) = (1342)$$

Cycle Notation Composition



2^{nd} $\quad$ 1^{st}

$$(134)(24) = (1342)$$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$
- $(145)(123) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$
- $(145)(123) = (12345)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$
- $(145)(123) = (12345)$
- $(15)(245)(12) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$
- $(145)(123) = (12345)$
- $(15)(245)(12) = (14)(25)$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$
- $(145)(123) = (12345)$
- $(15)(245)(12) = (14)(25)$
- $(43)(251)(145) =$

Cycle Notation: Lots of Little Examples

Some examples from S_4 the set of permutations of four objects:

- $(12)(123) = (23)$
- $(123)(12) = (13)$
- $(12)(34) = (34)(12)$
- $(12)(23)(34) = (1234)$
- $(12)(13)(14) = (1432)$
- $(14)(13)(12) = (1234)$
- $(123)(345) = (12345)$
- $(145)(123) = (12345)$
- $(15)(245)(12) = (14)(25)$
- $(43)(251)(145) = (134)(25)$

Disjoint Cycles

Theorem

Every permutation can be written as a product of disjoint cycles.

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:
So we get

$$\begin{aligned}(43)(251)(145) &= (a_1 \\ &= (1\end{aligned}$$

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:

- $a_2 = \sigma(a_1) = \sigma(1) = 3$

So we get

$$(43)(251)(145) = (a_1 a_2$$
$$= (13$$

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:

- $a_3 = \sigma(a_2) = \sigma(3) = 4$

So we get

$$\begin{aligned}(43)(251)(145) &= (a_1 a_2 a_3 \\ &= (134\end{aligned}$$

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j,$ *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:

- $\sigma(a_3) = \sigma(4) = 1$

So we get

$$\begin{aligned}(43)(251)(145) &= (a_1 a_2 a_3)\\ &= (134)\end{aligned}$$

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:

- $a_4 = 2$

So we get

$$\begin{aligned}(43)(251)(145) &= (a_1 a_2 a_3)(a_4 \\ &= (134)(2\end{aligned}$$

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:

- $a_5 = \sigma(a_4) = \sigma(2) = 5$

So we get

$$\begin{aligned}(43)(251)(145) &= (a_1 a_2 a_3)(a_4 a_5 \\ &= (134)(25\end{aligned}$$

Disjoint Cycles

Proof.

Given a permutation $\sigma \in S_n$ of the values $1, 2, 3, \ldots, n$, let $a_1 = 1$, then for all i

- if $\sigma(a_i) \neq a_j$, *for* $j \leq i$: let $a_{i+1} = \sigma(a_i)$ be the next element in the current cycle
- else: close the current cycle, let a_{i+1} be an element not already in a cycle

Repeat this until all the values $1, 2, 3, \ldots, n$ are used. The iterative definition insures that any new cycles will be equal or are disjoint. Since the new cycles are defined using σ it is the same permutation. □

Let $\sigma = (43)(251)(145)$ and $a_1 = 1$:

- $\sigma(a_5) = \sigma(5) = 2$

So we get

$$\begin{aligned}(43)(251)(145) &= (a_1 a_2 a_3)(a_4 a_5)\\ &= (134)(25)\end{aligned}$$

2-Cycles

Theorem

Every permutation can be written as a product of 2-cycles.

Proof.

Suppose that $\sigma = (a_1 a_2 a_3 \cdots a_k)$, then it can be "easily" checked that σ may be written in either of the following ways:

- $\sigma = (a_1 a_2)(a_2 a_3)(a_3 a_4) \cdots (a_{k-2} a_{k-1})(a_{k-1} a_k)$ or
- $\sigma = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$.

These two representations may be connected with the observation that:

$$(a_i a_j) = (a_i a_k)(a_k a_j)(a_i a_k),$$

e.g. $(14) = (13)(34)(13)$. □

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$(123)(45)(13) = (12)(23)(45)(13)$$

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$\begin{aligned}(123)(45)(13) &= (12)(23)(45)(13) \\ &= (12)\color{orange}{(23)}\color{black}(13)(45)\end{aligned}$$

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$\begin{aligned}(123)(45)(13) &= (12)(23)(45)(13)\\ &= (12)(23)(13)(45)\\ &= (12)(13)(12)(13)(13)(45)\end{aligned}$$

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$\begin{aligned}(123)(45)(13) &= (12)(23)(45)(13)\\ &= (12)(23)(13)(45)\\ &= (12)(13)(12)(13)(13)(45)\\ &= (12)(13)(12)(45)\end{aligned}$$

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$\begin{aligned}
(123)(45)(13) &= (12)(23)(45)(13) \\
&= (12)(23)(13)(45) \\
&= (12)(13)(12)(13)(13)(45) \\
&= (12)(13)(12)(45) \\
&= (12)(12)(23)(12)(12)(45)
\end{aligned}$$

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$\begin{aligned}(123)(45)(13) &= (12)(23)(45)(13)\\ &= (12)(23)(13)(45)\\ &= (12)(13)(12)(13)(13)(45)\\ &= (12)(13)(12)(45)\\ &= (12)(12)(23)(12)(12)(45)\\ &= (23)(12)(12)(45)\end{aligned}$$

Cycle Notation: A Useful Example

Shuffling 2-cycles to move a number left:

$$\begin{aligned}(123)(45)(13) &= (12)(23)(45)(13)\\ &= (12)(23)(13)(45)\\ &= (12)(13)(12)(13)(13)(45)\\ &= (12)(13)(12)(45)\\ &= (12)(12)(23)(12)(12)(45)\\ &= (23)(12)(12)(45)\\ &= (23)(45)\end{aligned}$$

Cycle Notation: Some Key Observations

- $(ac) = (ab)(bc)(ab)$

Cycle Notation: Some Key Observations

- $(ac) = (ab)(bc)(ab)$
- $(ac)(ac) = e$

Cycle Notation: Some Key Observations

- $(ac) = (ab)(bc)(ab)$
- $(ac)(ac) = e$
- $(ab)(cd) = (cd)(ab)$

Cycle Notation: Some Key Observations

- $(ac) = (ab)(bc)(ab)$
- $(ac)(ac) = e$
- $(ab)(cd) = (cd)(ab)$
- $(ab)(ac) = (ab)(ab)(bc)(ab) = (bc)(ab)$

Cycle Notation: Some Key Observations

- $(ac) = (ab)(bc)(ab)$
- $(ac)(ac) = e$
- $(ab)(cd) = (cd)(ab)$
- $(ab)(ac) = (ab)(ab)(bc)(ab) = (bc)(ab)$
- $(ac)(bc) = (bc)(ab)(bc)(bc) = (bc)(ab)$

Even and Odd Permutations

Lemma

Whenever it is written as a product of 2-cycles, the identity permutation is always a product of an even number of 2-cycles.

Even and Odd Permutations

Lemma

Whenever it is written as a product of 2-cycles, the identity permutation is always a product of an even number of 2-cycles.

Theorem

When written as a product of 2-cycles, every permutation is always either a product of an even number or of an odd number of 2-cycles, but not both.

Even and Odd Permutations

Lemma

Whenever it is written as a product of 2-cycles, the identity permutation is always a product of an even number of 2-cycles.

Theorem

When written as a product of 2-cycles, every permutation is always either a product of an even number or of an odd number of 2-cycles, but not both.

Theorem

The set of all even permutations, A_n (the ***alternating group****), is a subgroup of S_n.*

Even and Odd Permutations

Lemma

Whenever it is written as a product of 2-cycles, the identity permutation is always a product of an even number of 2-cycles.

Theorem

When written as a product of 2-cycles, every permutation is always either a product of an even number or of an odd number of 2-cycles, but not both.

Theorem

The set of all even permutations, A_n (the **alternating group***), is a subgroup of S_n.*
(Which is proved with the 2-Step Subgroup Test.)

Groups and Subgroups

Dr. Chuck Rocca

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES