Groups and symmetries

Tuesday, June 29, 2021 3:29 PM

Meta-example. Suppose X is any object. By a symmetry of X we mean a bijective function $f: X \to X$ which preserves properties of X. Let $\mathrm{Sym}(X)$ be the set of all symmetries of X. Notice that if $f, g: X \to X$ are two symmetries of X, then their composite $f \circ g$ should be also a symmetry of X. (at this point, think about this only intuitively.) Hence $\circ$ defines an operation on $\mathrm{Sym}(X)$. Since $(f \circ g) \circ h = f \circ (g \circ h)$, $\circ$ is associative. The identity function $\mathrm{id}_X : X \to X$ clearly preserves properties of X, and so $\mathrm{id}_X \in \mathrm{Sym}(X)$. Notice that, for every $f \in \mathrm{Sym}(X)$, $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$. Finally if $f: X \to X$ is a symmetry, then its inverse $f^{-1}: X \to X$ is also a symmetry. Notice that $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}_X$. Hence every element has an inverse. Therefore $(\mathrm{Sym}(X), \circ)$ is a group.

Next we will discuss a couple of special cases of the above meta-example in details.

Symmetric group

Tuesday, June 29, 2021 3:29 PM

We start with the case where X is just a non-empty set with no extra property. Then every bijection $f: X \to X$ is considered a symmetry of X. This takes us to the definition of the symmetric group of a set X.

<u>Def.</u> Suppose X is a non-empty set. Let

$$S_X := \{ f: X \to X \mid f \text{ is a bijection} \}.$$

For a positive integer n, let $S_n := S_{[1..n]}$ where

$$[1..n] := \{1, 2, \ldots, n\}.$$

<u>Proposition</u>. $(S_X, \circ)$ is a group where $f \circ g$ is the composition of f and g. (($S_X, \circ$) is called the symmetric group of X.)

<u>Pf.</u> We know that composite of two bijections is a bijection (if you do not remember this statement, try to prove it!)

Hence $\circ$ defines an operation on S_X. Notice that for every $f, g, h \in S_X$ and $x \in X$, we have

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) \quad \text{and}$$

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))). \text{ Therefore}$$

Symmetric group

Tuesday, June 29, 2021 3:29 PM

$(f\circ g)\circ h = f\circ(g\circ h)$. Therefore $\circ$ is associative.

. The identity function $id_X : X \to X$ is a bijection, and so $id_X \in S_X$. For every $f\in S_X$, $id_X \circ f = f\circ id_X = f$. Therefore id_X is the neutral element of S_X.

. Since $f: X\to X$ is a bijection, it is an invertible function (why?). Hence there is $f^{-1}: X\to X$ such that

$$f\circ f^{-1} = f^{-1}\circ f = id_X. \quad (\mathrm{I})$$

(I) implies that f^{-1} is an invertible function. Hence f^{-1} is a bijection (Here we are using the following result from set theory: $f: X\to Y$ is a bijection if and only if it is invertible.

It is a good exercise to reprove this result on your own.)

Therefore $f^{-1}\in S_X$. By (I), we deduce that $f^{-1}\in S_X$ is the inverse of f in $(S_X,\circ)$. ∎

<u>Def.</u> A group $(G,\cdot)$ is called abelian if for every $g_1,g_2\in G$, $g_1\cdot g_2 = g_2\cdot g_1$.

<u>Ex.</u> $(\mathbb{Z},+)$, $(\mathbb{Z}_n^\times,\cdot)$, $(\mathbb{C},+)$, and $(\mathbb{C}\setminus\{0\},\cdot)$ are abelian.

Symmetric group

Tuesday, June 29, 2021 3:29 PM

<u>Ex.</u> S_n is not abelian if $n \geq 3$.

<u>Pf.</u> Let $f_1 : [1..n] \to [1..n]$, $f_1(1) = 2$, $f_1(2) = 1$, and

$f_1(i) = i$ for $3 \leq i \leq n$.

Let $f_2 : [1..n] \to [1..n]$, $f_2(1) = 3$, $f_1(3) = 1$, and

$f_2(i) = i$ for $i \in [1..n] \setminus \{1, 3\}$.

Then clearly f_1 and f_2 are bijections, and so $f_1, f_2 \in S_n$.

$(f_1 \circ f_2)(1) = f_1(f_2(1)) = f_1(3) = 3$ and

$\neq$

$(f_2 \circ f_1)(1) = f_2(f_1(1)) = f_2(2) = 2$. Hence

$f_1 \circ f_2 \neq f_2 \circ f_1$. Therefore S_n is not abelian. ∎

Notice that elements of S_n are just permutations of $1, \ldots, n$.

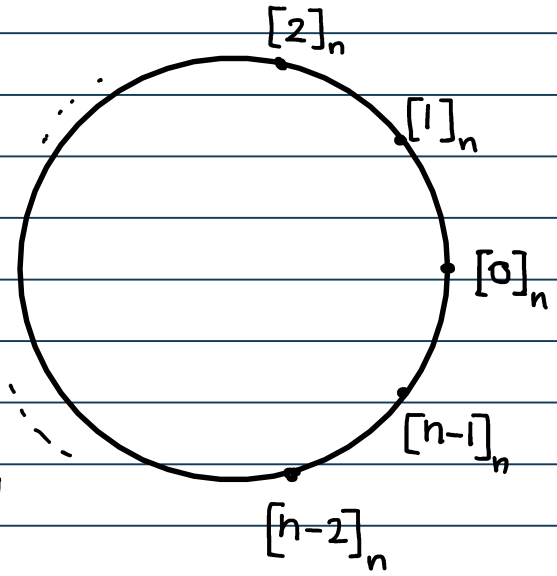
This means for $f(1)$ we have n choices, after choosing $f(1)$, for $f(2)$ we have exactly $n-1$ choices ($[1..n] \setminus \{f(1)\}$), and so on. Therefore there are $n(n-1) \cdots (2)(1)$ possibilities for f. Hence $|S_n| = n!$.

Next we consider symmetries of an n-cycle. An n-cycle is a graph with n vertices and n edges as we see in

Dihedral group

Tuesday, June 29, 2021 3:29 PM

the following figure.



We label the vertices by elements of $\mathbb{Z}_n$ to make our arguments more concrete.

As we can see $[i]_n$ is connected to exactly two vertices $[i-1]_n$ and $[i+1]_n$.

- A symmetry of a graph $\mathcal{G}$ with the set of vertices V is the set of bijections $f: V \to V$ such that for every $v, w \in V$, $\{v, w\}$ is an edge if and only if

$$\{f(v), f(w)\} \text{ is an edge.}$$

Following the meta-example one can check that the set of symmetries of a graph $\mathcal{G}$ with composition $\circ$ is a group.

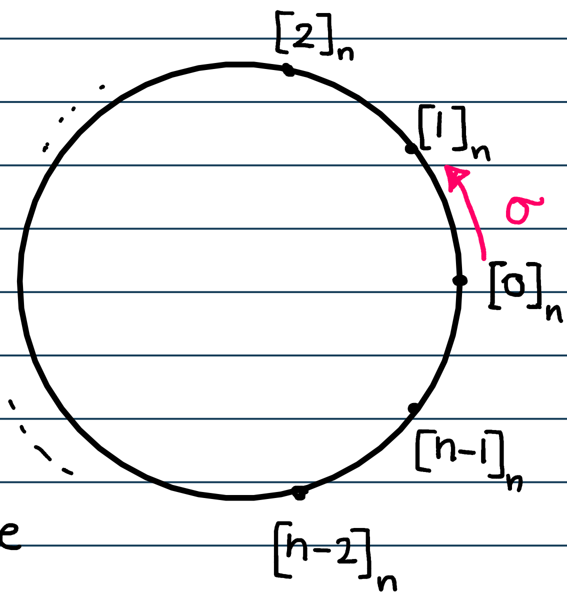
Here we would like to understand the group of symmetries of an n-cycle.

- First we notice that every vertex looks like other vertices.

This means we can send $[0]_n$ to any other vertex using a

Dihedral group

Tuesday, June 29, 2021 3:29 PM



symmetry. Consider the rotation by one step; that means

$\sigma: \mathbb{Z}_n \to \mathbb{Z}_n$, $\sigma(x) := x + [1]_n$.

Notice that σ is a bijection as $x \mapsto x + [-1]_n$ is the inverse of σ. We also notice that $\sigma(x) - \sigma(y) = x - y$, and x is connected to y exactly when $x - y \in \{[1]_n, [-1]_n\}$. Hence $\{x, y\}$ is an edge if and only if $\{\sigma(x), \sigma(y)\}$ is an edge. Therefore σ is a symmetry of this graph.

Notice that $\sigma^i(x) = \sigma \circ \cdots \circ \sigma(x)$

$$= (\cdots(x + \underbrace{[1]_n) + [1]_n) + \cdots) + [1]_n}_{i \text{ times}}$$

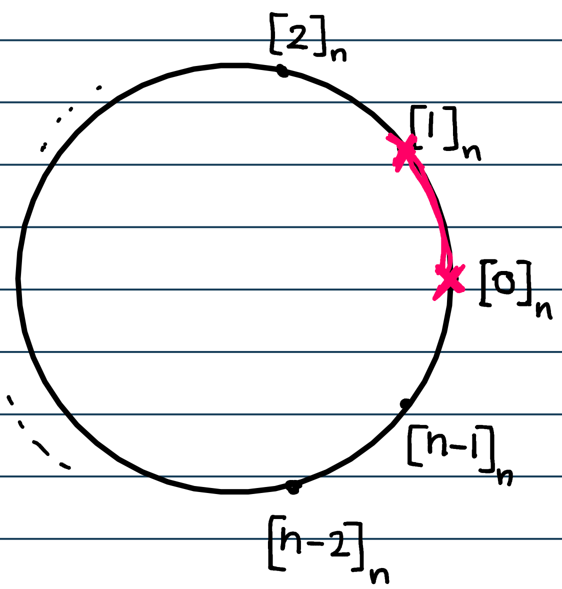
Hence $\sigma^i(x) = x + [i]_n$. In particular, $\sigma^i([0]_n) = [i]_n$.

Next we want to see what we say about symmetries that do not move $[0]_n$. Suppose γ is a symmetry and $\gamma([0]_n) = [0]_n$. Since $[1]_n$ is connected to $[0]_n$, $\gamma([1]_n)$ is connected to

Dihedral group

Tuesday, June 29, 2021 3:29 PM

$\gamma([0]_n) = [0]_n$. This means $\gamma([1]_n)$ is either $[1]_n$ or $[-1]_n$.



<u>Claim.</u> If γ is a symmetry of the n-cycle, $\gamma([0]_n) = [0]_n$, and $\gamma([1]_n) = [1]_n$, then $\gamma = \mathrm{id}$.

<u>Pf.</u> We prove by strong induction on i that $\gamma([i]_n) = [i]_n$.

By hypothesis, we know that this is true for $i = 0$ and 1.

Suppose $\gamma([i]_n) = [i]_n$ for $0 \le i \le k$ and $k \ge 1$.

We want to show that $\gamma([k+1]_n) = [k+1]_n$.

Notice that, since $[k]_n$ is connected to $[k+1]_n$, $\gamma([k]_n)$ is connected to $\gamma([k+1]_n)$. Because $\gamma([k]_n) = [k]_n$, $\gamma([k+1]_n)$ is either $[k-1]_n$ or $[k+1]_n$. Since $0 \le k-1 \le k$, by the strong induction hypothesis, $\gamma([k-1]_n) = [k-1]_n$. Because γ is a bijection and $\gamma([k+1]_n) \neq \gamma([k-1]_n)$ unless $[k+1]_n = [k-1]_n$. If $[k+1]_n = [k-1]_n$, then

$\gamma([k+1]_n) = \gamma([k-1]_n) = [k-1]_n = [k+1]_n$. If $[k+1]_n \neq [k-1]_n$,

Dihedral group

Tuesday, June 29, 2021 3:29 PM

then $\gamma([k+1]_n) \neq \gamma([k-1]_n)$,

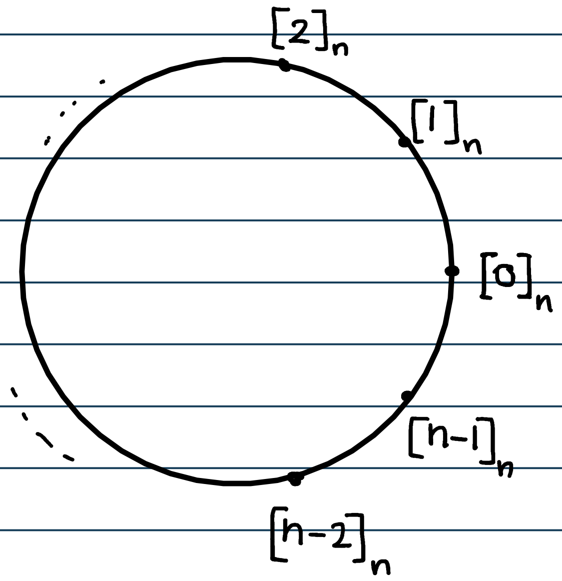
which means $\gamma([k+1]_n) \neq [k-1]_n$.

Because $\gamma([k+1]_n)$ is either

$[k-1]_n$ or $[k+1]_n$, and it is not

$[k-1]_n$, we conclude that

$\gamma([k+1]_n) = [k+1]_n$. The claim follows. ∎



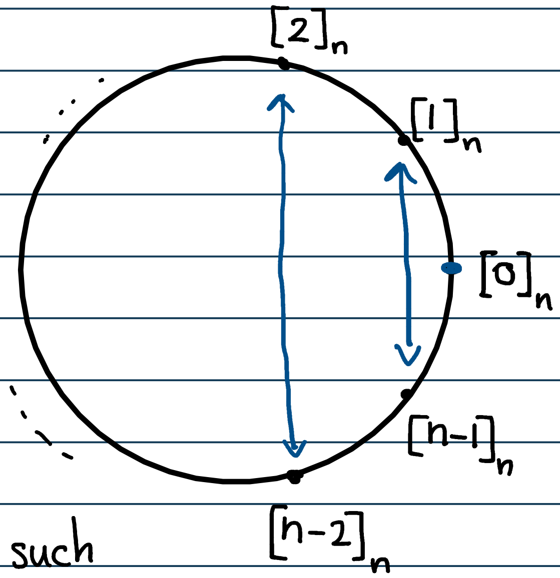
To understand symmetries

which fix $[0]_n$ and send $[1]_n$

to $[-1]_n$, we notice that

the reflection,

$\tau: \mathbb{Z}_n \to \mathbb{Z}_n$, $\tau(x) := -x$ is such



a symmetry. Notice that, for every $x, y \in \mathbb{Z}_n$,

$\tau(x) - \tau(y) = y - x$. Hence $x - y \in \{[1]_n, [-1]_n\}$ if and

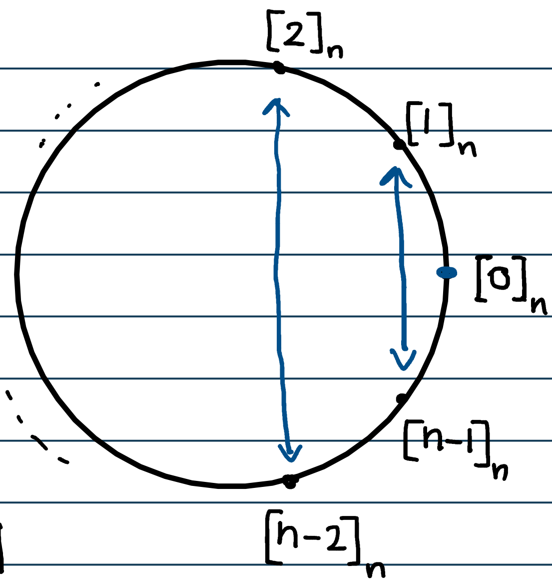
only if $\tau(x) - \tau(y) \in \{[1]_n, [-1]_n\}$. This means x is

connected to y if and only if $\tau(x)$ is connected to $\tau(y)$.

We also notice that $\tau^2 = id$, and so τ is a bijection.

Dihedral group

Tuesday, June 29, 2021 3:29 PM



Therefore τ is a symmetry of the n-cycle, $\tau([0]_n)=[0]_n$, and $\tau([1]_n)=[-1]_n$.

<u>Claim</u>. If γ is a symmetry of the n-cycle, $\gamma([0]_n)=[0]_n$, and $\gamma([1]_n)=[-1]_n$, then $\gamma=\tau$.

<u>Pf</u>. Consider the symmetry $\tau\circ\gamma$. Notice that

$$\tau\circ\gamma([0]_n)=\tau(\gamma([0]_n))=\tau([0]_n)=[0]_n \text{ and}$$

$$\tau\circ\gamma([1]_n)=\tau(\gamma[1]_n)=\tau([-1]_n)=[1]_n.$$

By the 1st claim, $\tau\circ\gamma=\text{id}$. Hence

$$\tau\circ(\tau\circ\gamma)=\tau\circ\text{id} \Rightarrow \underbrace{(\tau\circ\tau)}_{\text{id.}}\circ\gamma=\tau$$

$$\Rightarrow \gamma=\tau.$$

Now we can describe all the symmetries of the n-cycle.

<u>Theorem</u>. The group of symmetries of the n-cycle graph whose vertices are labelled by elements of $\mathbb{Z}_n$ consists of $\{\text{id}, \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\circ\tau, \ldots, \sigma^{n-1}\circ\tau\}$ where $\sigma:\mathbb{Z}_n\to\mathbb{Z}_n$

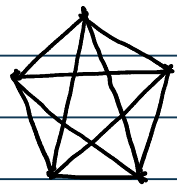
Dihedral group

Tuesday, June 29, 2021 3:29 PM

$\sigma(x) = x + [1]_n$ (rotation) and $\tau: \mathbb{Z}_n \to \mathbb{Z}_n$, $\tau(x) = -x$.
(reflection)

<u>Pf.</u> Suppose γ is a symmetry of this graph. Suppose $\gamma([0]_n) = [i]_n$. Then $\gamma([0]_n) = \sigma^i([0]_n)$, and so $\sigma^{-i} \circ \gamma$ is a symmetry which stabilizes $[0]_n$; that means $\sigma^{-i} \circ \gamma([0]_n) = [0]_n$. We have showed that there are exactly two such symmetries: id. and τ. Hence $\sigma^{-i} \circ \gamma = \mathrm{id.}$ or $\sigma^{-i} \circ \gamma = \tau$. Multiplying both sides of these equations by σ^i from left, we obtain that either $\gamma = \sigma^i$ or $\gamma = \sigma^i \circ \tau$. This completes the proof. ∎

From the previous theorem, in particular we deduce that the n-cycle graph has $2n$ symmetries. The symmetric group can be viewed as the group of symmetries of the complete graph K_n with n vertices.



K_5

The common idea for finding the number of symmetries of these graphs is the following:

An idea for symmetries of a graph

Tuesday, June 29, 2021 3:29 PM

1. Start with a vertex v_1 and find out how many other vertices look like v_1. (A symmetry can send v_1 to those vertices)
2. Take one of the neighbors v_2 of v_1 and find out after fixing v_1 how many of the neighbors of v_1 look like v_2.
3. Continue the above process till you reach to a rigidity; this means if a symmetry fixes $v_1, v_2, \dots, v_k$, then it is identity.
4. Multiply all the numbers that you have found!