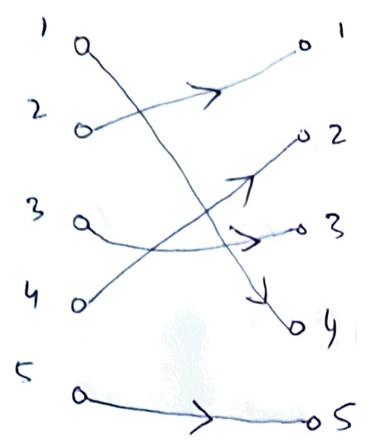
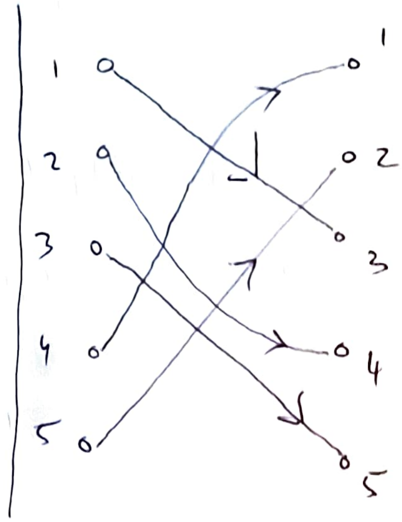
Let's look at permutations closely:

Let's consider two permutations of $\{1,2,3,4,5\}$:



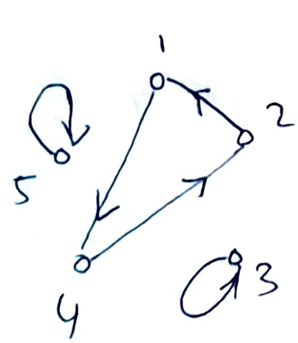


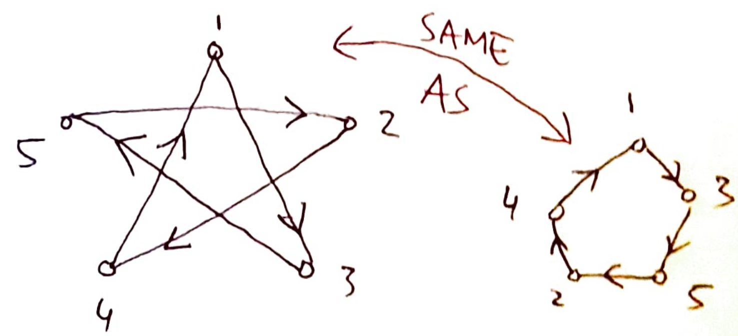
And let us represent/visualize them in different ways:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} \quad \text{two row/line format} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

For a permutation of S: In the first line, we write elements of S in some order. In the second line, we write the image of each element (in first line) below it.

Now let us represent as a digraph on the set $\{1,2,3,4,5\}$:





In both cases, we got a directed graph (on 5 vertices) that is just a collection of vertex-disjoint dicycles.

Is this a coincidence? NO!

DIY: Prove the following:

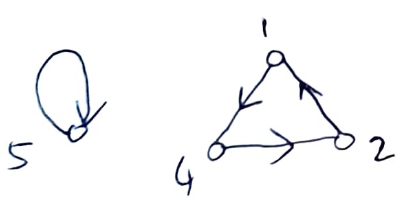
(1) Let D be a finite digraph where each vtx v has $d^{in}(v) = d^{out}(v) = 1$. Then D is simply a collection of vtx-disjoint dicycles.

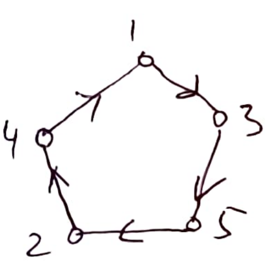
↳ means any two distinct dicycles can NOT share any vertex ⇒ they can NOT share any arc either

(2) Every permutation on a finite set S can be represented as a collection of vertex-disjoint dicycles on the set S.

↓

This leads us to the cycle representation of permutations:





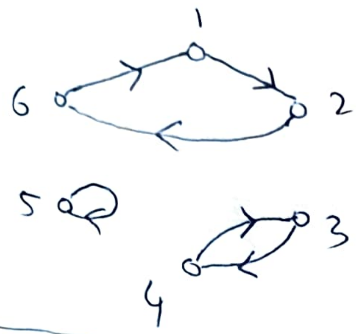
$(5)(1\ 4\ 2)(3)$

$(1\ 3\ 5\ 2\ 4)$

This is called the $\boxed{\text{cycle representation}}$ of a permutation.

CS1200 Module-3: Counting & Algebraic Structures

One more example: a permutation of $\{1,2,3,4,5,6\}$



cycle representation

2-line format:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 3 & 5 & 1 \end{pmatrix}$$

It turns out that the set of permutations of a set S has some "nice" properties — that are similar to some other sets you/we are already familiar with — for example, the set of integers along with the addition (+) operation.

↓

Let us compare these two "sets"

↓

Before that we need to decide what is our "addition" operation for permutations (of a set)

↓

Question: Can you think of an operation that takes two permutations & "combines them" to produce another permutation?

Answer: Function composition $(\circ)$
(defined/discussed in Module-1)

CS1200 Module-3: Counting & Algebraic Structures

$(\mathbb{Z}, +)$	set of all permutations of a set S $(\mathcal{S}, \circ)$ function composition operation
① addition of two integers $\in \mathbb{Z}$ produces another integer $\in \mathbb{Z}$ called CLOSURE property order does NOT matter $(a+b=b+a)$ order matters! ($f \circ g \neq g \circ f$ in general)	composition of two permutations f & g $(\in \mathcal{S})$ (in ~~some~~ this order) produces another permutation $f \circ g \in \mathcal{S}$ (DIY: prove)
② $a+(b+c) = (a+b)+c$ called ASSOCIATIVITY	$f \circ (g \circ h) = (f \circ g) \circ h$ $\forall f, g, h \in \mathcal{S}$ (DIY: prove)
③ $0+x = x+0 = x \quad \forall x \in \mathbb{Z}$ (identity: 0) called EXISTENCE of IDENTITY element	$f \circ i = i \circ f = f \quad \forall f \in \mathcal{S}$ where i is the identity bijection/permutation (identity: i) (DIY: prove)
④ $x + (-x) = (-x) + x = 0 \quad \forall x \in \mathbb{Z}$ (inverse of x: $-x$) called EXISTENCE of INVERSE	$f \circ f^{-1} = f^{-1} \circ f = i \quad \forall f \in \mathcal{S}$ (DIY: prove) (inverse of f: f^{-1})

This brings us to our first algebraic structures:

a set with some (1 or more) special operations that together satisfy some "nice" properties.

GROUP:

A $\boxed{\text{group}}$ is a nonempty set Γ (Gamma) together with a binary operation, say $\bullet$ (aka group operation) that combines any two elements, say a & b (in that order), of Γ to form an element $\boxed{\text{of } \Gamma}$ denoted $a \bullet b$, such that the following hold:

CLOSURE property

① Associativity:

$\forall a, b, c \in \Gamma: \ (a \bullet b) \bullet c = a \bullet (b \bullet c)$

② Existence of Identity Element:

$\exists$ an element $e \in \Gamma$ such that $\forall a \in \Gamma$:

$e \bullet a = a$ AND $a \bullet e = a$.

③ Existence of Inverse:

$\forall a \in \Gamma, \exists b \in \Gamma$ such that $a \bullet b = e$ AND $b \bullet a = e$.

Thus, as per definition on previous page, we have seen two examples of groups:

1. $(\mathbb{Z}, +)$ — an infinite group since $\mathbb{Z}$ is infinite
2. $(\mathcal{S}, \circ)$ ——— finite group if S is finite; otherwise infinite

$\mathcal{S}$: the set of permutations of a set S

In particular, if $S = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N} - \{0\}$ then $\mathcal{S}_n$ denotes the set of all permutations of S, and is commonly known as the **symmetric group of order n.**

plays a very important role in group theory — a topic of study in abstract algebra with many applications to computer science (especially, but NOT limited to, cryptography).

Why care about group theory?

One can prove some very general results in group theory that can be applied to specific groups to prove/deduce cool results — similar to how we used poset theory (Dilworth's Theorem) to prove Erdos-Szekeres Theorem.