Symmetric Groups

Prepared by Mark on March 31, 2026

Instructor's Handout
This handout contains solutions and notes.
Recompile without solutions before distributing.

Section 1: Introduction

Definition 1:
Informally, a *permutation* on a collection of n objects is an ordering of these n objects.
For example, a few permutations of `A`, `B`, `C`, and `D` are `ABCD`, `BCDA`, and `DACB`.

This, however, isn't the definition we'll use today. Instead of defining permutations as "ordered lists" (like we do above), we'll define them as *functions* on finite sets.
Our first goal today is to make sense of this definition.

Definition 2: Permutations
Let Ω be a set of n arbitrary objects.
A *permutation* f on Ω is a map[1] from Ω to itself that produces a *unique* output for each input.
This means that if a and b are different, $f(a)$ and $f(b)$ must also be different.

For example, consider $\{1, 2, 3\}$.
One permutation on this set can be defined as follows:

- $f(1) = 3$
- $f(2) = 1$
- $f(3) = 2$

If we take the array 123 and apply f, we get 312.

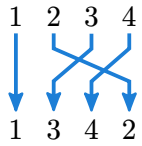
Problem 3:
List all permutations on three objects.
How many permutations of n objects are there?

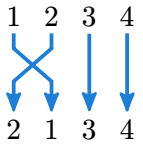
Problem 4:
What map corresponds to the permutation that produces the array `312` from the array `123`?

Problem 5:
What map corresponds to the "do-nothing" permutation?
Write it as a function and in square-bracket notation.
We will call this the *trivial permutation*

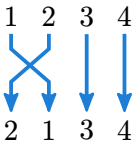
[1] The words "function" and "map" are equivalent.

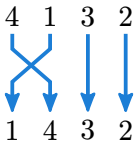
We can visualize a permutation using a *string diagram*. The arrows in this diagram denote the output of f for each possible input. Two examples are below:

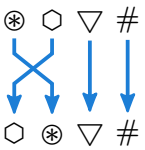




Note that the elements of the set we are permuting are not ordered. (it is a *set*, after all!)
For example, consider the diagrams below. On the left, 1234 are ordered as usual.
In the middle, they are ordered alphabetically.
The rightmost diagram uses arbitrary, meaningless labels.







It shouldn't be hard to see that despite the different "output" each diagram displays (2134, 1432, and ⬡ ⊛ ▽ #), the same permutation ("swap first two") is shown in each.
Observe the following:

- The "names" of the items in our set do not have any meaning.
  We are interested in sets of n arbitrary things, which we may label however we like.
- Permutations are *verbs*.
  We do not care about the "output" of a certain permutation. Rather, we care about what it *does*.
  We could, for example, describe the permutation in the above three diagrams as "swap the first two elements."

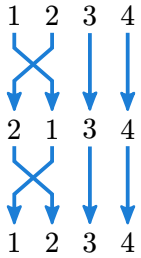
Definition 6: Square Brackets
However, elements with an implicit order (1, 2, 3, …) are convenient.
Such sets let us denote a permutation by writing the array it produces after transforming the "reference order" 123...n.
We will call this *square-bracket notation*.
[312] denotes the permutation that produces 312 when applied to 123.

Problem 7:
Draw string diagrams for [4123] and [2341].

Section 2: Cycle Notation

Definition 8: Order
The *order* of a permutation f is the smallest positive n where $f^n(x) = x$ for all x.
In other words, if we repeatedly apply a permutation with order n,
we will get back to where we started after n steps.

For example, consider [2134]. This permutation has order 2, as we can see below:



Swapping the first two elements of a list twice changes nothing.
Thus, [2134] has an order of two.

Problem 9:
What is the order of [2314]?
How about [4321]?
Note: Try to solve this problem without drawing any strings!

Problem 10:
Find a permutation on five elements with order 4.

Problem 11:
Show that all permutations on a finite set have a well-defined order.
In other words, show that there must always be an integer n where $f^n(x) = x$.

Definition 12: Composition
The *composition* of two permutations f and g is the permutation $h(x) = f(g(x))$.
We'll denote this by simply writing the permutations we're composing next to each other, like fg.
Note that g is applied *before* f in fg.

Problem 13:
Show that function composition is associative.
That is, show that $f(gh) = (fg)h$.

Problem 14:
What is [1324][4321]?
How about [321][213][231]?
Rewrite these compositions as one permutation in square brackets.

Solution:

- [1324][4321] is [4321]
- [321][213][231] is [123]

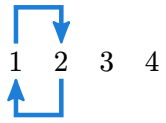
As you may have noticed, the square-bracket notation we've been using thus far is a bit unwieldy.
Permutations are verbs—but we've been referring to them using a noun (i.e, their output).
Square-bracket notation fails to capture the structure of the permutation it identifies.

Is the permutation [1234] different than the permutation [12345]?
These permutations operate on different sets—but they are both the identity!
Are [5342761] and [1342567][5234761] similar? What are their orders?

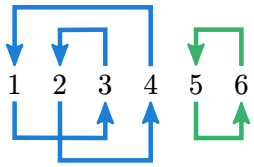
Good notation should help us understand the objects we are studying.
We need something better than square brackets.

Remark 15: Cycles
Any permutation is composed of a number of *cycles*.
Reread Problem 11 to convince yourself of this fact.

Example 16:
Consider the permutation [2134].
It consists of one two-cycle: $1 \to 2 \to 1$, which we can see in the diagram below.
Note: $3 \to 3$ and $4 \to 4$ are also cycles, but we'll ignore them. One-cycles aren't interesting.



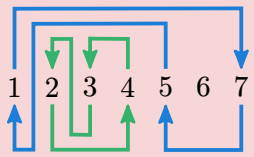
The permutation [431265] is a bit more interesting—it contains two cycles:



Remark 17:
Two-cycles may also be called *transpositions*.
Any permutation that swaps two elements is a transposition.

Problem 18:
Find all cycles in [5342761].

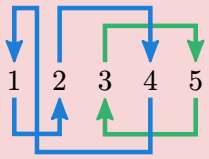
Solution:



There are two non-trivial cycles:
- $4 \to 3 \to 2 \to 4$
- $1 \to 7 \to 5 \to 1$

Problem 19:
What permutation on five objects is formed by the cycles $3 \to 5 \to 3$ and $1 \to 2 \to 4 \to 1$?
Write it in square-bracket notation.

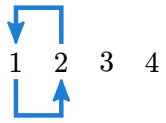
Solution:



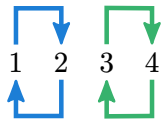
This is [41523].

Definition 20: Cycle Notation
We can use cycles to develop better notation:
Instead of identifying permutations using their output, we'll identify them using their *cycles*.

For example, we'll write [2134] is (12) in cycle notation,
since it consists only of the cycle $1 \to 2 \to 1$:



Permutations that consist of more than one cycle are written as a composition.
[2143] is written as (12)(34). Applying the permutation [2143] has the same effect as applying (34), then applying (12).

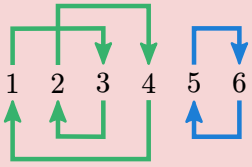


Remark 21:
According to Problem 11, any permutation may be written as a composition of disjoint cycles.
Convince yourself of this fact.

Problem 22:
Rewrite [431265] in cycle notation.

Solution:

[431265] is (1324)(56):



Remark 23:
The identity permutation $f(x) = x$ is written as () in cycle notation.

Problem 24:
Convince yourself that disjoint cycles commute.
That is, that (1324)(56) = (56)(1324) = [431265] since (1324) and (56) do not overlap.

Problem 25:
Write the following in square-bracket notation.

- (12) on a set of 2 elements
- (12)(435) on a set of 5 elements
- (321) on a set of 3 elements
- (321) on a set of 6 elements
- (1234) on a set of 4 elements
- (3412) on a set of 4 elements

Note that (12) refers the "swap first two" permutation on a set of *any* size.
We can use consistent notation for the same action on two different sets!

Problem 26:
Write the following in square-bracket notation. Pay attention!

- (13)(243) on a set of 4 elements
- (243)(13) on a set of 4 elements

Problem 27:
Consider the last two permutations in Problem 25, (1234) and (3412).
These are *identical*—they are the same cycle written in two different ways.
List all other ways to write this cycle.
Hint: There are two more.

Definition 28: Inverse
The *inverse* of a permitation f is a permutation g that "un-does" f.
This means that $g(f(x)) = x$ for all x.

Problem 29:
What is the inverse of (12)?
How about (123)? And (4231)?
Note we do not need to know the size of the set we are operating on.
The inverse of (12) is the same in sets of all sizes!

Problem 30:
Let σ be a permutation composed of disjoint cycles $\sigma_1\sigma_2...\sigma_k$.
Say we know the order of all σ_i. What is the order of σ?

Solution:

$$\text{lcm}(\text{ord}(\sigma_1),\ \text{ord}(\sigma_2),\ ...,\ \text{ord}(\sigma_k))$$

Problem 31:
Show that any cycle $(123...n)$ is equal to the product $(12)(23)...(n-1,n)$.

Solution:

Intuition:
$(123...n)$ is a right-shift. Swapping all pairs from right to left achieves the same effect.

Complete solution:
Consider $n-1$. After applying $(123...n)$, it takes the position of n.
After applying $(n-1,n)$, $n-1$ moves to the same position *and is never moved again!*
Repeat this argument for all other n.

Problem 32:
Write (7126453) as a product of transpositions.

Solution:

Move elements one at a time, and using the last position as temporary storage.
We get (71)(72)(76)(74)(75)(73). Other solutions are possible.

Bonus: How can we do this in the fewest number of transpositions?

Problem 33:
Show that any permutation is a product of transpositions.

Solution:

Re-use the argument in Problem 31.
Pick an arbitrary "working slot," and re-build all cycles.
Use the "not touched again" argument for a proper proof.

Problem 34:
Show that any permutation is a product of transpositions of the form $(1, k)$.

Solution:

Use Problem 33 to rewrite each (a, b) as $(1, a)(1, b)(1, a)$.
Showing that $(a, b) = (1, a)(1, b)(1, a)$ is fairly easy.

Problem 35:
Show that any transposition (a, b) is equal to the product $(a, a+1)(a+1, b)(a, a+1)$.

Solution:

This is the same as Problem 34, but we use $a+1$ as a "working slot" instead of 1.

Problem 36:
Show that any permutation is a product of adjacent transpositions.
An *adjacent transposition* swaps two adjacent elements, and thus looks like $(n, n+1)$.

Solution:

As before, we will use Problem 33 and rewrite the transpositions it produces in a convenient fashion. To do this, we must show that every transposition (a, b) is a product of adjacent transpositions.

In the proof below, assume that $a < b$ and perform induction on $b - a$.

Base Case:
If $b - a = 1$, (a, b) is a product of adjacent transpositions.
In fact, it *is* an adjacent transposition.

Induction:
Now, say $b - a = n + 1$.
Assume that all (a, b) where $b - a \leq n$ are products of adjacent transpositions.
By Problem 35, $(a, b) = (a, a+1)(a+1, b)(a, a+1)$.

$(a, a+1)$ is an adjacent transposition, and $b - (a+1) = n$.
Thus, (a, b) is a product of adjacent transpositions.

Section 3: Groups (review)

Definition 37:
Before we continue, we must introduce a bit of notation:

- S_n is the set of permutations on n objects.
- $\mathbb{Z}_n$ is the set of integers mod n.
- $\mathbb{Z}_n^\times$ is the set of integers mod n with multiplicative inverses.
  In other words, it is the set of integers smaller than n and coprime to n.[2]
  For example, $\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$.

Problem 38:
What are the elements of S_3? *Hint:* Use cycle notation
How about $\mathbb{Z}_{17}^\times$?

Definition 39:
A *group* $(G, *)$ consists of a set G and an operator $*$.
Groups always have the following properties:

1. G is closed under $*$. In other words, $a, b \in G \Rightarrow a * b \in G$.
2. $*$ is *associative*: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
3. There is an *identity* $e \in G$, so that $a * e = e * a = a$ for all $a \in G$.
4. For any $a \in G$, there exists a $b \in G$ so that $a * b = b * a = e$. b is called the *inverse* of a.
   This element is written as $-a$ if our operator is addition and a^{-1} otherwise.

Any pair $(G, *)$ that satisfies these properties is a group.

Problem 40:
Is $(\mathbb{Z}_5, +)$ a group?
Is $(\mathbb{Z}_5, -)$ a group?
$+$ and $-$ refer to the usual operations in modular arithmetic.

Problem 41:
What is the group with the fewest number of elements?

Solution:

Let $(G, \star)$ be our group, where $G = \{x\}$ and $\star$ is defined by $x \star x = x$
Verifying that the trivial group is a group is trivial.

[2] We proved this in another handout, but you may take it as fact here.

Problem 42:
Show that function composition is associative

Problem 43:
Show that S_n is a group under composition.

Problem 44:
Let $(G, *)$ be a group with finitely many elements, and let $a \in G$.
Show that there is an n in $\in \mathbb{Z}^+$ so that $a^n = e$
Hint: $a^n = a * a * ... * a$ repeated n times.

The smallest such n defines the *order* of g.
Hint: We've already done a special case of this problem!
Find it in this handout, then rewrite your proof for an arbitrary (finite) group.

Problem 45:
What is the order of 5 in $(\mathbb{Z}_{25}, +)$?
What is the order of 2 in $(\mathbb{Z}_{17}^{\times}, \times)$?

Definition 46: Generator
Let G be a group, and let g be an element of G.
We say g is a *generator* if every other element of G may be written as a power of g.

Problem 47:
Let G be a group of n elements.
If g is a generator, what is its order?
Provide a proof.

Problem 48:
Find the two generators in $(\mathbb{Z}, +)$
Then, find all generators of $(\mathbb{Z}_5, +)$

Problem 49:
How many groups have only one generator?

Solution:

Only one: the trivial group. The inverse of a generator is also a generator!

Definition 50:
Let S be a subset of the elements in G.
We say that S *generates* G if every element of G may be written as a product of elements in S.
Note: This is an extension of Definition 46.

Problem 51:
We've already found a few generating sets of S_n. What are they?

Solution:

The following sets generate S_n:

- All transpositions
- All transpositions of the form $(1, k)$
- All adjacent transpositions

The smallest generating set of S_n consists of the transposition (12) and the n-cycle $(1, 2, ..., n)$.
The proof of this is a bonus problem later in the handout.

Section 4: Subgroups

Problem 52:
What elements do S_2 and S_3 share?

Consider the sets $\{1, 2\}$ and $\{1, 2, 3\}$. Clearly, $\{1, 2\} \subset \{1, 2, 3\}$.
Can we say something similar about S_2 and S_3?

Looking at Problem 52, we may want to say that $S_2 \subset S_3$ since every element of S_2 is in S_3.
This however, isn't as interesting as it could be. Remember that S_2 and S_3 are *groups*, not *sets*: their elements come with structure, which the "subset" relation does not capture.

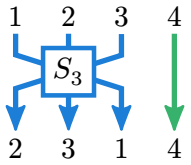
To account for this, we'll define a similar relation: subgroups.

Definition 53: Subgroup
Let G and G' be groups. We say G' is a *subgroup* of G (and write $G' \subset G$) if the following are true:
(Note that x, y are elements of G, and xy is multiplication in G)

- the set of elements in G' is a subset of the set of elements in G.
- the identity of G is in G'
- $x, y \in G' \Rightarrow xy \in G'$
- $x \in G' \Rightarrow x^{-1} \in G'$

The above definition may look fairly scary, but the idea behind a subgroup is simple.
Consider S_3 and S_4, the groups of permutations of 3 and 4 elements.

Say we have a set of four elements and only look at the first three.
S_3 fully describes all the ways we can arrange those three elements:



Problem 54:
Show that S_3 is a subgroup of S_4.

Definition 55: Isomorphism
Let G and H be groups. We say that G and H are *isomorphic* (and write $G \cong H$) if there is a bijection $f : G \to H$ with the following properties:

- $f(e_G) = e_H$, where e_G is the identity in G
- $f(x^{-1}) = f(x)^{-1}$ for all x in G
- $f(xy) = f(x)f(y)$ for all x, y in G

Intuitively, you can think of isomorphism as a form of equivalence.
If two groups are isomorphic, they only differ by the names of their elements.
The function f above tells us how to map one set of labels to the other.

Problem 56:
Show that $\mathbb{Z}_7^\times$ and $\mathbb{Z}_9^\times$ are isomorphic. *Hint:* Build a bijection with the above properties. Remember that a group is fully defined by its multiplication table.

Problem 57:
Show that $\mathbb{Z}_{10}^\times$, $\mathbb{Z}_5^\times$, and $\mathbb{Z}_4$ are isomorphic. *Hint:* Build a bijection with the above properties. Remember that a group is fully defined by its multiplication table.

Problem 58:
Show that isomorphism is transitive.
That is, if $A \cong B$ and $B \cong C$, then $A \cong C$.

Problem 59:
How many subgroups of S_4 are isomorphic to S_3?

Problem 60:
What are the orders of S_3 and S_4?
How is this related to Problem 59?

Solution:

$|S_4| = |S_3| \times [S_4 : S_3]$

This solution is written using index notation,
but the class doesn't need to know what it means yet.

Problem 61:
S_4 also has S_2 and the trivial group as subgroups.
How many instances of each does S_4 contain?

Problem 62:
$(\mathbb{Z}_4, +)$ is also a subgroup of S_4. Find it!
How many subgroups of $\mathbb{Z}_4$ are isomorphic to S_4?

Solution:

A good hint is "look at generators."

There are four instances of $\mathbb{Z}_4$ in S_4, each of which is generated by a 4-cycle of S_n.
(i.e, the group generated by (1234) is isomorphic to $\mathbb{Z}_4$)

Section 5: Bonus problems

Problem 63:
Show that $x \in \mathbb{Z}^+$ has a multiplicative inverse mod n iff $\gcd(x, n) = 1$

Problem 64:
Let $\sigma = (\sigma_1\sigma_2...\sigma_k)$ be a k-cycle in S_n, and let τ be an arbitrary element of S_n.
Show that $\tau\sigma\tau^{-1} = (\tau(\sigma_1), \tau(\sigma_2), ..., \tau(\sigma_k))$
Hint: τ is a permutation, so $\tau(x)$ is the value at position x after applying τ.

Problem 65:
Show that the set $\{(1, 2), (1, 2, ..., n)\}$ generates S_n.