Symmetric Groups

Prepared by Mark on April 3, 2024

Part 1: Introduction

Definition 1:
Let Ω be an arbitrary set of n objects.
A *permutation* on Ω is a bijective map $f : \Omega \to \Omega$.

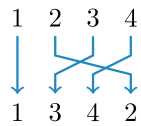
For example, consider the objects 1, 2, and 3.
The permutation [312] is given by a map f defined by the following table:
- $f(1) = 3$
- $f(2) = 1$
- $f(3) = 2$

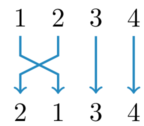
Problem 2:
List all permutations on three objects.
How many permutations of n objects are there?

Problem 3:
What map corresponds to the permutation [321]?

Problem 4:
What map corresponds to the "do-nothing" permutation?
Write it as a function and in square-bracket notation.
Note: We usually call this the *trivial permutation*

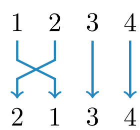
We can visualize permutations with a *string diagram*, shown below.
The arrows in this diagram denote the image of f for each possible input. Two examples are below:

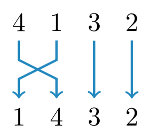


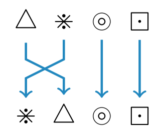


Note that in all our examples thus far, the objects in our set have an implicit order. This is only for convenience. The elements of Ω are not ordered (it is a *set*, after all), and we may present them however we wish.

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" order (2134 and 1432),
the same permutation is depicted in all three diagrams. This example demonstrates two things:

- First, the names of the items in our set do not have any meaning.
  Ω is just a set of n arbitrary things, which we may label however we like.
- Second, permutations are verbs. We do not care about the "output" of a certain permutation, we care about what it *does*. We could, for example, describe the permutation above as "swap the first two of four elements."

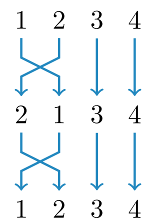
Why, then, do we order our elements when we talk about permutations? As noted before, this is for convenience. If we assign a natural order to the elements of Ω (say, 1234), we can identify permutations by simply listing their output: Clearly, [1234] represents the trivial permutation, [2134] represents "swap first two," and [4123] represents "cycle right."

Problem 5:
Draw string diagrams for [4123] and [2341].

Part 2: Cycle Notation

Definition 6: Order
The *order* of a permutation f is the smallest positive n so that $f^n(x) = x$ for all x.
In other words: if we repeat this permutation n times, we get back to where we started.
Note that the order is given by the *smallest* positive integer n. There may be more than one!

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



Of course, swapping the first two elements of a list twice changes nothing.
Thus, [2134] is its own inverse, and has an order of two.
Naturally, the identity permutation has order one.

Problem 7:
What is the order of [2314]?
How about [4321]?
Note: You shouldn't need to draw any strings to solve this problem.

Problem 8: Bonus
Show that all permutations (on a finite set) have a well-defined order.
In other words, show that there is always an integer n so that $f^n(x) = x$.

Definition 9: Composition
The *composition* of two permutations f and g is the permutation $h(x) = f(g(x))$.
The usual notation for this is $f \circ g$, but we'll simply write fg.

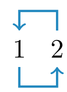
Problem 10:
What is [1324][4321]?
How about [321][213][231]?
Hint: is composition is left or right-associative? See Definition 9

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 (namely, their output when applied to an ordered sequence of numbers). Our notation fails to capture the meaning of the underlying object.

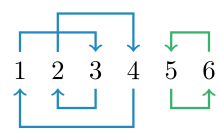
Think about it: is the permutation [1234] different than the permutation [12345]?
Indeed, these permutations operate on different sets—but they are both the identity!
What should we do if we want to talk about the identity on $\{1, 2, ..., 10\}$?

We need something better.

Definition 11: Cycles
Any permutation is composed of a number of *cycles*.
For example, consider the permutation [2134], which consists of one two-cycle: $1 \to 2 \to 1$
Note: $3 \to 3$ and $4 \to 4$ are also cycles, but we'll ignore them. One-cycles aren't aren't interesting.



The permutation [431265] is a bit more interesting—it contains of two cycles:
($1 \to 3 \to 2 \to 4 \to 1$ and $5 \to 6 \to 5$)



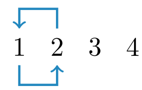
Another name we'll often use for two-cycles is *transposition*.
Any permutation that swaps two adjacent elements is called a transposition.

Problem 12:
Find all cycles in [5342761].

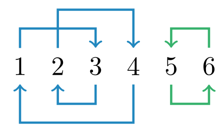
Problem 13:
What permutation (on five objects) is formed by the cycles $3 \to 5 \to 3$ and $1 \to 2 \to 4 \to 1$?

Definition 14: Cycle Notation
We now have a solution to our problem of notation. Instead of referring to permutations using their output, we will refer to them using their *cycles*.

For example, we'll write [2134] as (12), which denotes the cycle $1 \to 2 \to 1$:



As another example, [431265] is (1324)(56) in cycle notation.
Note that we write [431265] as a *composition* of two cycles:
applying the permutation [431265] is the same as applying (1324), then applying (56).



Any permutation σ may be written as a product (i.e, composition) of disjoint cycles $\sigma_1\sigma_2...\sigma_k$.
Make sure you believe this fact. If you don't, ask an instructor.
Also, the identity $f(x) = x$ is written as () in cycle notation.

Problem 15:
Convince yourself that disjoint cycles commute.
That is, that $(1324)(56) = (56)(1324) = [431265]$ since (1324) and (56) do not overlap.

Problem 16:
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 now use the same name for the same permutation on two different sets!

Problem 17:
Write the following in square-bracket notation. Be careful.

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

Problem 18:
Look at the last two permutations in Problem 16, (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.
Also, note that the last two permutations in Problem 16 are the same.

Problem 19:
What is the inverse of (12)?
How about (123)? And (4231)?
Note that again, we don't need to know how big our set is.
The inverse of (12) is the same in all sets.

Problem 20:
Say σ is 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?

Problem 21:
Show that any cycle $(123...n)$ is equal to the product $(12)(23)...(n-1, n)$.

Problem 22:
Write (7126453) as a product of transpositions.

Problem 23:
Show that any permutation is a product of transpositions.

Problem 24:
Show that any permutation is a product of transpositions of the form $(1, k)$.

Problem 25:
Show that any transposition (a, b) is equal to the product $(a, a+1)(a+1, b)(a, a+1)$.

Problem 26:
Show that any permutation is a product of adjacent transpositions.
(An *adjacent transposition* swaps two adjacent elements, and thus looks like $(n, n+1)$)

Part 3: Groups (review)

Definition 27:
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.[1]
  For example, $\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$.

Problem 28:
What are the elements of S_3? *Hint:* Use cycle notation
How about $\mathbb{Z}_{17}^\times$?

Definition 29:
A *group* $(G, *)$ consists of a set G and an operator $*$.
Groups always have the following properties:

A: G is closed under $*$. In other words, $a, b \in G \implies a * b \in G$.
B: $*$ is *associative*: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
C: There is an *identity* $e \in G$, so that $a * e = a * e = a$ for all $a \in G$.
D: 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 30:
Is $(\mathbb{Z}_5, +)$ a group?
Is $(\mathbb{Z}_5, -)$ a group?
Note: $+$ and $-$ refer to the usual operations in modular arithmetic.

Problem 31:
What is the group with the fewest elements?

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

Problem 32:
Show that function composition is associative

Problem 33:
Show that S_n is a group under composition.

Problem 34:
Let $(G, *)$ be a group with finitely many elements, and let $a \in G$.
Show that $\exists n \in \mathbb{Z}^+$ so that $a^n = e$
Hint: $a^n = a * a * ... * a$ repeated n times.

The smallest such n defines the *order* of g.

Example Solution

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 35:
What is the order of 5 in $(\mathbb{Z}_{25}, +)$?
What is the order of 2 in $(\mathbb{Z}_{17}^\times, \times)$?

Definition 36:
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 37:
Say the size of a group G is n.
If g is a generator, what is its order?
Provide a proof.

Problem 38:
Find the two generators in $(\mathbb{Z}, +)$
Then, find all generators of $(\mathbb{Z}_5, +)$

Problem 39:
How many groups have only one generator?

Definition 40:
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 that this is an extension of Definition 36.

Problem 41:
We've already found a few generating sets of S_n. What are they?

Part 4: Subgroups

Problem 42:
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 42, 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.

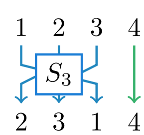
To account for this, we'll define a similar relation: subgroups.

Definition 43:
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'
- $x, y \in G' \implies xy \in G'$
- $x \in G' \implies x^{-1} \in G'$

The above definition may look faily 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 44:
Show that S_3 is a subgroup of S_4.

Definition 45:
Let G and H be groups. We say that G and H are *isomorphic* (and write $A \simeq B$) 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 46:
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 47:
Show that $\mathbb{Z}_{10}^\times$ and $\mathbb{Z}_5^\times$, 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 48:
Show that isomorphism is transitive.
That is, if $A \simeq B$ and $B \simeq C$, then $A \simeq C$.

Problem 49:
How many subgroups of S_4 are isomorphic to S_3?

Problem 50:
What are the orders of S_3 and S_4?
How is this related to Problem 49?

Problem 51:
S_4 also has S_2 and the trivial group as subgroups.
How many instances of each does S_4 contain?

Problem 52:
$(\mathbb{Z}_4, +)$ is also a subgroup of S_4. Find it!
How many subgroups of $\mathbb{Z}_4$ are isomorphic to S_4?.

Part 5: Bonus problems

Problem 53:
Show that $x \in \mathbb{Z}^+$ has a multiplicative inverse mod n iff $\gcd(x, n) = 1$

Problem 54:
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 $\tau \sigma \tau^{-1} = \big(\tau(\sigma_1), \tau(\sigma_2), ..., \tau(\sigma_k)\big)$
Hint: As usual, τ is a permutation. Thus, $\tau(x)$ is the value at position x after applying τ.

Problem 55:
Show that the set $\Big\{(1, 2),\ (1, 2, ..., n)\Big\}$ generates S_n.