Lecture 3: Permutations: An Introduction

Contents

The puzzles we have encountered so far all have a common theme: the pieces can be mixed up, and the goal is to restore the pieces back to some proper order. In this lecture we will introduce some terminology and notation for talking about rearrangements of objects. In particular, we give the definition of a *permutation*, which is the main object we will use to study puzzles. We'll also discuss *permutation multiplication*, *inverses*, and *order*.

This lecture corresponds to Sections 2.1, 3.1, 3.2 or Joyner's text.

3.1 Permutation: Preliminary Definition

In mathematics, the notion of *permutation* is used with several slightly different meanings, all related to the act of permuting (rearranging in an ordered fashion) objects or values. Informally, a permutation of a set of objects is an arrangement of those objects into a particular order.

Example 3.1 *There are six permutations of the objects in the set* $\{1, 2, 3\}$*, namely* $[1, 2, 3]$*,* $[1, 3, 2]$*,* $[2, 1, 3]$*,* $[2, 3, 1]$*,* $[3, 1, 2]$*, and* $[3, 2, 1]$.

Notation: Curly braces $\{,\}$ denote *sets*, i.e. the order that elements are listed doesn't matter. Square braces $[,]$ denote lists, i.e. the order that elements appear does matter. So as sets $\{1,2,3\} = \{2,1,3\}$ but as lists $[1,2,3] \neq [2,1,3]$.

SAGE

```
sage: Set([1,2,3])==Set([2,1,3])
True
sage: [1,2,3]==[2,1,3]
False
```

Example 3.2 *There are* 5040 *ways to arrange the seven books in the Harry Potter series on your bookshelf. If we let* 1 *denote Volume 1: Philosopher's Stone,* 2 *denote Volume 2: Chamber of Secrets, etc. then, for example, two possible permutaions are* $[1,3,5,7,2,4,6]$ *and* $[5,2,1,3,7,4,6]$. *Of course, out of all these possible permutations one is likely to place them in order on their bookshelf:* $[1,2,3,4,5,6,7]$.

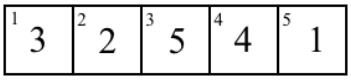
To determine the number of permutations we imagine 7 *empty slots on the bookshelf which we are about to fill. There are* 7 *ways to pick a book and place it in slot* 1. *For each of these choices, there are now* 6 *possible ways to fill slot* 2, *then* 5 *possible ways to fill slot* 3, *etc. So the total number of ways to fill the* 7 *slots is:* $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 7! = 5040$.

SAGE

```
sage: factorial(7)
5040
```

Example 3.3 *In the game of Swap on* 5 *objects the empty puzzle board is shown in Figure 1a.*

(a) The empty Swap board



(b) A random arrangement of Swap.

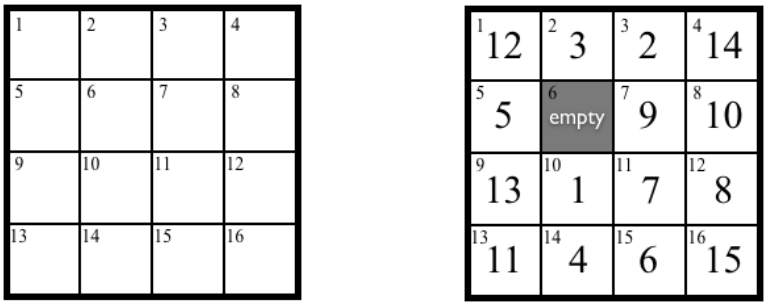
Figure 1: Game of Swap

The puzzle board is filled by laying out the tiles numbered 1 *through* 5 *in the boxes. For example, one such puzzle position is shown in Figure 1b. Each puzzle position corresponds to a permutation of the set* $\mathbb{Z}_5 = \{1,2,3,4,5\}$. *There are* $5! = 120$ *permutations of* $\mathbb{Z}_5$, *and so there are* 120 *different possible positions in the game of Swap. Only one of which is the solved state.*

Example 3.4 *The fifteen puzzle with no tiles in the boxes is shown in Figure 2a.*

The puzzle is started by placing the 15 *tiles anywhere on the board. For example, one such puzzle position is shown in Figure 2b. This corresponds to a permutation of the set* $\mathbb{Z}_{16}$, *where we imagine the blank space as being the* 16^{th} *tile. There are* $16! = 20,922,789,888,000$ *permutations of* $\mathbb{Z}_{16}$, *and so there are* $16!$ *different ways to lay the tiles on the board. As for which positions are actually solvable, well this is a question we will investigate later.*

We can use SAGE to generate permutations of a list, for example $[1,2,3]$.



(a) The empty 15-Puzzle board

(b) A random arrangement of the 15-Puzzle.

Figure 2: The 15 Puzzle

SAGE

```
sage: terms=[1,2,3];
sage: Permutations(terms)
Permutations of the set [1, 2, 3]
sage: Permutations(terms).list();
[[1, 2, 3], [1, 3, 2], [2, 1, 3], [2, 3, 1], [3, 1, 2], [3, 2, 1]]
sage: number_of_permutations(terms)
6
sage: factorial(3)
6
```

Sometimes when listing permutations of a set we will omit the square braces. For example the 6 permutations of $[1,2,3]$ can be listed as: $123, 132, 213, 231, 312, 321$.

We can also list permutations of a multi-set, that is a set with more than one element repeated. Though, to define a multi-set we would actually need to use a list.

Example 3.5 *Two permutations of the multi-set* $[a,a,b,b,b]$ *are* $[b,a,b,a,b]$ *and* $[b,b,a,a,b]$. *There are* $\frac{5!}{2!\cdot 3!} = 10$ *permutations in total. (Since there are* $5!$ *ways to arrange* 5 *objects, but* 2 *of the objects are identical, and so are the other* 3*.)*

SAGE

```
sage: var('a,a,b,b,b');
sage: terms=[a,a,b,b,b];
sage: Permutations(terms)
Permutations of the multi-set [a, a, b, b, b]
sage: Permutations(terms).list();
[[a, a, b, b, b], [a, b, a, b, b], [a, b, b, a, b], [a, b, b, b, a], [b,
a, a, b, b], [b, a, b, a, b], [b, a, b, b, a], [b, b, a, a, b], [b, b,
a, b, a], [b, b, b, a, a]]
sage: number_of_permutations(terms)
10
sage: factorial(3)/(factorial(2)*factorial(3))
10
```

3.2 Permutation: Mathematical Definition

It will be convenient for us to have a slightly more mathematical definition of a permutation. Before we give this formal definition of a *permutation* we start by recalling the notion of a *function*, and the properties: *one-to-one*, and *onto*.

3.2.1 Functions

Definition 3.1 *A **function**, or **mapping**, f from a (nonempty) set A to a (nonempty) set B is a rule that associates each element $a \in A$ to exactly one element $b \in B$.*

Notation & Terminology: We write $f : A \to B$ to denote a function named f from set A to set B. A is called the **domain** of f and B the **codomain**. If f sends a to b then we write $f(a) = b$, or $f : a \mapsto b$. We also say b is the **image** of a under f. The subset of B consisting of all images $f(a)$, for $a \in A$, is called the **range** of f, and is written:

$$f(A) = \{f(a) \mid a \in A\} \subset B.$$

See Figure 3 for a pictorial representation of these ideas.

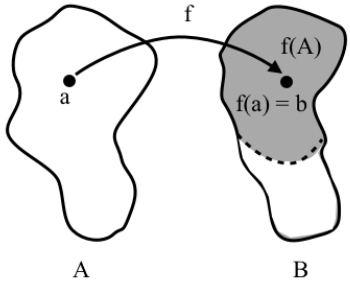


Figure 3: The way to visualize a function, domain, codomain and range.

Definition 3.2 *A function $f : A \to B$ is called **one-to-one**, or **injective**, if each element of B appears at most once as the image of an element of A.*

*A function $f : A \to B$ is called **onto**, or **surjective**, if $f(A) = B$. That is, if each element of B is the image of at least one element of A.*

*A function that is both injective and surjective is called **bijective**.*

3.2.2 Permutations

Now for the definition of a permutation.

Definition 3.3 *A **permutation** of a set A is a function $\alpha : A \to A$ that is bijective (i.e. both one-to-one and onto).*

Our goal is to understand how the pieces of a puzzle move around, so we typically represent each piece by a number, that is by an element of $\mathbb{Z}_n = \{1, 2, 3, \ldots, n\}$. A rearrangement of the pieces then corresponds to a bijection from $\mathbb{Z}_n \to \mathbb{Z}_n$, a *permutation* as defined above.

Unlike in calculus, where most function are defined on infinite sets and given by formulas, permutations of finite sets are usually given by simply listing where each value goes.

For example, we can define a permutation α of the set $\{1, 2, 3\}$ by stating:

$$\alpha(1) = 2, \quad \alpha(2) = 1, \quad \alpha(3) = 3.$$

In SAGE we can use the `Permutation()` command to construct a permutation. Here we define the permutation by the list of images $[\alpha(1), \alpha(2), \ldots]$.

SAGE

```
sage: a=Permutation([2,1,3]); a
[2,1,3]
sage: a(1)
2
sage: a(2)
1
```

A slightly more convenient way to represent this permutation is by:

$$\alpha \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

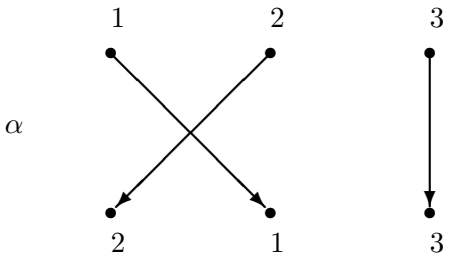
where the top row are the element of $\mathbb{Z}_3$ and the bottom row are the corresponding images under α. This is known as *array notation* for a permutation.

Here is an example of how to use matrices in SAGE to display a permutation in array form. One way is to use the `matrix()` command, where the syntax is
`matrix( [ <list for row 1> , <list for row 2> ] ).`

SAGE

```
sage: a=Permutation([2,1,3])
sage: matrix([[1,2,3],[a(i) for i in [1,2,3]]]);
[1 2 3]
[2 1 3]
```

A more visual representation is by mean of an *arrow diagram*. The arrows point from x to $\alpha(x)$.



Array Notation: We may define a permutation $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ by a $2 \times n$ array:

$$\alpha \leftrightarrow \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}.$$

Since α is bijective the second row would just be a rearrangement of the numbers in the top row.

Example 3.6

*(a) The **identity** permutation, denoted by ε, or I, is the permutation that does nothing:*

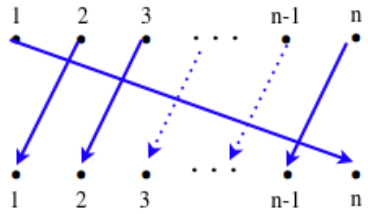
$$\varepsilon \leftrightarrow \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

It may not seem obvious why we would want to consider the "do nothing" permutation, but we will consider this permutation quite a bit. As an analogy, think about 0, this is a symbol which represents "nothing" but yet appears almost everywhere in mathematics.

*(b) An **n- cycle** is a permutation which cyclically permutes the values. For example,*

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ n & 1 & 2 & \dots & n-1 \end{pmatrix}.$$

We could also visualize this with an arrow diagram:



Every number moves to the right and the last one, n, cycles around back to to 1.

3.3 Composing Permutations

Now that we have some basic notations for permutations we can now look at how to combine two permutations in order to produce a third one. The method we use is called *composition*. This will be precisely the tool we will need in order to understand how two puzzle moves combine together to give a third.

Let α and β be two permutations of $\mathbb{Z}_n$. We wish to define a new function $\alpha \circ \beta : \mathbb{Z}_n \to \mathbb{Z}_n$, called the *permutation composition*. In order to define a function on $\mathbb{Z}_n$ we just need to specify how it maps the elements. For $k \in \mathbb{Z}_n$ we'll define $(\alpha \circ \beta)(k)$ to be the result of first applying α, then applying β to the result. In other words,

$$(\alpha \circ \beta)(k) = \beta(\alpha(k)), \text{ for } k \in \mathbb{Z}_n.$$

This new function is again a permutation. To see why we just need to observe that it is a bijection.

Injective: Suppose $(\alpha \circ \beta)(k) = (\alpha \circ \beta)(\ell)$ for some $k, \ell \in \mathbb{Z}_n$, then $\beta(\alpha(k)) = \beta(\alpha(\ell))$ implies $\alpha(k) = \alpha(\ell)$, since β is one-to-one. It follows that $k = \ell$ since α is one-to-one. Therefore, $\alpha \circ \beta$ is one-to-one.

Surjective: Consider any $m \in \mathbb{Z}_n$. Let $\ell \in \mathbb{Z}_n$ such that $\beta(\ell) = m$, and let $k \in \mathbb{Z}_n$ such that $\alpha(k) = \ell$. Both ℓ and k exist since α and β are onto. It follows that $(\alpha \circ \beta)(k) = \beta(\alpha(k)) = m$. Therefore, $\alpha \circ \beta$ is onto. This verifies that $\alpha \circ \beta$ is a permutation.

This way of combing permutations will essentially underline everything we do in this course so we should make this a formal definition. We will also drop the symbol $\circ$ to simplify writing.

Definition 3.4 *Let $\alpha, \beta : \mathbb{Z}_n \to \mathbb{Z}_n$ be two permutations. The **permutation composition**, or **product**, of α and β is denoted by $\alpha\beta : \mathbb{Z}_n \to \mathbb{Z}_n$ is the permutation defined by:*

$$\begin{array}{rccccc} \alpha\beta: & \mathbb{Z}_n & \to & \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & k & \longmapsto & \alpha(k) & \longmapsto & \beta(\alpha(k)) \end{array}$$

Important: Notice that the composition is opposite to the way functions were combined in calculus. In calculus, and in most branches of mathematics, there is a long standing tradition that variables are to appear to the right of the function: $f(x)$. The composition, $(f \circ g)(x)$ is then read from right-to-left: $f(g(x))$. So why are we defining the composition of permutations as *left-to-right*, and going against long standing mathematical tradition? Well, there is a good reason for this. Imagine you were asked to apply the move sequence R $\mathrm{F}^{-1}$to a Rubik's cube. What move would you do first, R or F^{-1}? Well, the popular convention is to read from left-to-right and apply R first, then F^{-1}. This is popular since, for example, this is how you are reading the words on the page right now, from left-to-right. This is precisely the convention we are taking to combine permutations, we combine them from left-to-right.

Example 3.7 *(a) Let* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$ *and* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$. *Then*

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}.$$

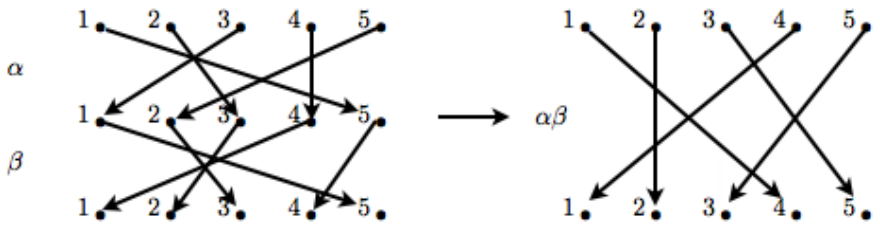
On the right we have 4 *under* 1, *since* $\alpha\beta(1) = \beta(\alpha(1)) = \beta(5) = 4$, *so* $\alpha\beta$ *sends* 1 *to* 4. *This is illustrated by following the arrows above. Notice the movement is from left-to-right, which is our chosen convention for composing two permutation. The other values are determined in a similar fashion.*

We can use SAGE *to multiply permutations.*

SAGE

```
sage: a=Permutation([5,3,1,4,2]);  a
[5, 3, 1, 4, 2]
sage: b=Permutation([5,3,2,1,4]); b
[5,3,2,1,4]
sage: a*b
[4, 2, 5, 1, 3]
```

We can also use the arrow diagram representation for permutations to give us more visual insight into how permutations are composed:



If we compose α and β in the other order, we find

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}.$$

This shows that permutation composition is not commutative in general. That is, we typically have $\alpha\beta \neq \beta\alpha$.

SAGE

```
sage:  b*a
[2, 1, 3, 5, 4]
```

(b) Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 8 & 1 & 4 & 5 & 6 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 6 & 7 & 8 & 3 & 4 \end{pmatrix}$. Then

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 8 & 1 & 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 6 & 7 & 8 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \varepsilon.$$

*Therefore $\alpha\beta$ is the identity permutation. Permutations with the property that their product is ε are called **inverse permutations**, since one permutation is undoing the rearrangement the other one performed.*

(c) For any permutation α we can take the product of α with itself: $\alpha\alpha$, we write this as α^2. In general we write the product of α with itself n-times, $\alpha\alpha\cdots\alpha$, as α^n.

Suppose $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ then the powers of α are:

$$\alpha^2 = \alpha\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}, \qquad \alpha^3 = \alpha\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

$$\alpha^4 = \alpha\alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}, \qquad \alpha^5 = \alpha\alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

$$\alpha^6 = \alpha\alpha^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Check these products yourself. We see that α^6 is the identity permutation. This raises the question: Can we always multiply a permutation to itself a finite number of times and end up with the identity permutation?

From the previous example two questions are raised:

(i) For any permutation α, must there exist a permutation β such that $\alpha\beta = \varepsilon$?

(ii) For any permutation α, must there exist a positive integer n such that $\alpha^n = \varepsilon$?

If we think about a permutation as a move on one of our puzzles, say Rubik's cube, then these questions are equivalent to asking: (i) When a move is applied, can it then be undone by another move? (ii) Applying the same move over and over again, will you eventually get back to where you started?

Phrased in this way, it may seem obvious that the answer is *yes* in both cases. For example, if the move F was applied (*clockwise* quarter turn of the front face), then the move F^{-1}undoes it (*counterclockwise* turn of the front face). Try this on your Rubik's cube. Moreover, for the move F, applying it 4 times in a row takes you back to where you started. This means F^4 is the identity, or *do-nothing move*. If the answer to the questions above is now obvious then you already have a working understanding of *inverses* and *orders*.

We'll discuss these topics in a little more detail over the next few sections. But first let's play with the cube a little more.

Exercise 3.1 *Consider Rubik's cube and the legal moves F, B, R, L, U, D, F^{-1}, B^{-1}, R^{-1}, L^{-1}, U^{-1}, D^{-1}, and all successive combinations of these moves.*

Recall a move sequence is read as follows: F U^{-2}means first twist the front face a quarter turn in the clockwise direction, then turn the up face a half turn in the counterclockwise direction.

(a) What is the inverse of the move sequence F U^{-2}? That is, if you apply move sequence F U^{-2}, then what is the sequence of moves which will undo this?

(b) How many times does the move sequence U^2 R^2 need to be applied in order to get you back to where you started? (Play with your cube to figure this out, and try not to lose count as you're twisting faces.)

3.4 Associativity of Permutation Composition

When adding and multiplying real numbers we don't need to worry about what to do first. For example, in the expression $2 \cdot 3 \cdot 4$ we get the same result if we multiply 2 and 3 first, then multiply the result by 4: $(2 \cdot 3) \cdot 4 = 6 \cdot 4 = 24$, as we get if we multiply 3 and 4 first, then multiply by 2: $2 \cdot (3 \cdot 4) = 2 \cdot 12 = 24$. This property of multiplication is called *associativity*, and it is written: $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{R}$.

What associativity means is that we can write the product of three (or more) numbers without having to use grouping brackets: abc. Since no matter which product you take first it will not affect the result.

The same is true for addition of real numbers: $(a + b) + c = a + (b + c)$. This means we can write $a + b + c$ without any confusion about which sum to perform first.

We have shown that we have a way to combine permutations. A fundamental question to ask is: Is permutation composition associative? That is, must we have $(\alpha\beta)\gamma = \alpha(\beta\gamma)$?

Well, permutation composition *is* associative. Lucky for us, this means we don't have to use group brackets when writing long chains of products. The reason that it is associative is simply because permutations are functions, and function composition is associative. To see this, consider permutations $\alpha, \beta, \gamma : \mathbb{Z}_n \to \mathbb{Z}_n$. For any $k \in \mathbb{Z}_n$,

$$((\alpha\beta)\gamma)(k) = \gamma((\alpha\beta(k)) = \gamma(\beta(\alpha(k))$$

and

$$(\alpha(\beta\gamma))(k) = (\beta\gamma)(\alpha(k)) = \gamma(\beta(\alpha(k)),$$

which are the same. [1] So $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

This means we can write $\alpha\beta\gamma$ for the product of these three permutations and there is no confusion about what product we should do first. The result won't change.

Example 3.8 *Let* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$, *and* $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$. *Then*

$$\begin{aligned}(\alpha\beta)\gamma &= \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}\right]\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \\ &= \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}\right]\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}\end{aligned}$$

and

$$\begin{aligned}\alpha(\beta\gamma) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}\left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}\right] \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}\left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}\right] \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}\end{aligned}$$

It shouldn't come as a surprise that we get the same result for $(\alpha\beta)\gamma$ *and* $\alpha(\beta\gamma)$. *This is what associativity means. We write this product as* $\alpha\beta\gamma$.

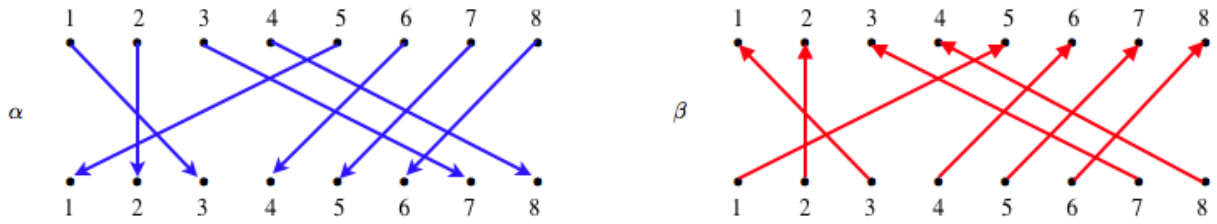
3.5 Inverses of Permutations

We saw in Example 3.7(b) permutations α and β such that the product was the identity: $\alpha\beta = \varepsilon$. We will call permutations with the property that their product is the identity, *inverses*. Let's look at this example a little more closely.

The permutations under consideration are:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 8 & 1 & 4 & 5 & 6 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 6 & 7 & 8 & 3 & 4 \end{pmatrix}.$$

We can represent α by an arrow diagram. Each blue arrow represents the mapping defined by the permutation α. If we replace each blue arrow with a red arrow pointing in the opposite direction then we get an arrow diagram representing β (follow arrows from bottom row to top row). In this sense, the inverse permutation is obtained by "reversing the arrows".



[1] Our convention is to compose permutations from left to right, see Definition 3.4.

We can do the same experiment with the array form of β. Let's flip β over, that is, we'll switch the top and bottom rows:

$$\begin{pmatrix} 5 & 2 & 1 & 6 & 7 & 8 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix},$$

then let's put the top row in increasing order, while keeping all the columns in tact:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 8 & 1 & 4 & 5 & 6 \end{pmatrix}.$$

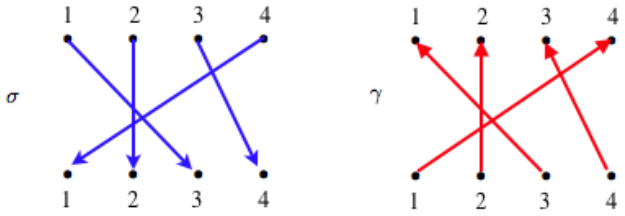
This precisely α! Should we be surprised this happened? What is really going on here?

To see what is going on, let's recall that the notation means the number in the top row maps to the number directly beneath it in the bottom row. For instance, α maps 1 to 3. If β is to be the inverse of α then it must undo what α does. In particular, it must map 3 back to 1. This means 3 must appear above 1 in the array from of β. Let's say this again: if 1 is above 3 in α, then 3 is above 1 in β.

The same is true for every number. In general, we have if k is above m in α (i.e. $\alpha(k) = m$) then m is above k in β (i.e. $\beta(m) = k$). This explains exactly what we observed when we flipped β.

Now suppose, we start with a permutation, say $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ and we flip the rows, and reorder the first row so it is increasing order, while keeping the columns in tact: $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. Is this a permutation? Well, each number from 1 to 4 appears in the second row, so it is surjective, and no number appears more than once, so it is injective. Therefore, yes, it is a permutation. And by the observation above, it is the inverse of σ, that is, $\sigma\gamma = \varepsilon$.

We can also use the arrow diagram to see this visually. γ was constructed by "reversing the arrows" of σ, so clearly γ is a bijection, and it is the inverse of σ, since it just undoes what σ is doing.



These observations tell us two things: every permutation has an inverse, and it is unique. Moreover, we have a straighforward way to construct inverses given a permutation in array or arrow form.

This result is so important that we state it as a theorem. We'll also give a formal proof of the theorem, which captures the essence of our discussion above in just a few lines.

Theorem 3.1 *For any permutation $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$, there exists a unique permutation $\beta : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $\alpha\beta = \beta\alpha = \varepsilon$.*

Proof: Let α be a permutation, define a new function $\beta : \mathbb{Z}_n \to \mathbb{Z}_n$ as follows:

$$\beta(m) = k \iff \alpha(k) = m$$

for $k, m \in \mathbb{Z}_n$. Since α is bijective, for any m such a k exists and is unique. It follows that $(\alpha\beta)(m) = \alpha(\beta(m)) = \alpha(k) = m$ and $(\beta\alpha)(k) = \beta(\alpha(k)) = \beta(m) = k$. This proves the theorem. □

Definition 3.5 *For any permutation α the unique permutation β such that $\alpha\beta = \beta\alpha = \varepsilon$ is called the **inverse** of α and is denoted by α^{-1}.*

Example 3.9 *Find the inverse of each of the following permutations. Verify it is the inverse by computing the product and showing it is the identity permutation.*

(a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$ *(b)* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

(a) The inverse of α can be obtained by reading the array form from the bottom row to the top row. For example, 1 in the bottom row must map to the number above it, which is 2. Similarly for the other numbers, so $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

SAGE *has a built-in* `inverese()` *command.*

SAGE
```
sage:  a=Permutation([3,1,2,5,4])
sage:  a.inverse()
[2, 3, 1, 5, 4]
```

(b) Similar to (a), we read the array form of β from bottom-to-top to get the array from of β^{-1}: $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. *Notice this is just β itself. So β is its own inverse.*

SAGE
```
sage:  b=Permutation([3,4,1,2])
sage:  b.inverse()
[3, 4, 1, 2]
```

3.5.1 Inverse of a Product

Apply the move sequence RU to your Rubik's cube. Now undo this move sequence. That is, return the cube to the state it was in before you apply RU. It is very likely you just applied the move sequence $\mathrm{U}^{-1}\,\mathrm{R}^{-1}$. If you did, then you have a working understanding of how to find the inverse of a product.

As another example, in the morning you get dressed you put on your *socks* then your *shoes*, but when you come home at night and get undressed you takes off your *shoes* then your *socks*. The order in which things are undone is opposite to which they were done.

If these two example seem obvious, it is because they in fact are. But even obvious things can be stated as theorems, which are just convenient summaries of observations for later use.

Theorem 3.2 *For two permutations α and β,*

$$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}.$$

In general, the inverse of a product permutations is the product of the inverses in the reverse order:

$$(\alpha_1\alpha_2\cdots\alpha_k)^{-1} = \alpha_k^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}.$$

Proof: Taking the product, and using associativity of permutation multiplication,

$$\begin{aligned}(\alpha\beta)(\beta^{-1}\alpha^{-1}) &= \alpha\beta\beta^{-1}\alpha^{-1}\\ &= \alpha\varepsilon\alpha^{-1}\\ &= \alpha\alpha^{-1}\\ &= \varepsilon\end{aligned}$$

Therefore, $\beta^{-1}\alpha^{-1}$ is the inverse of $\alpha\beta$. A similar argument proves the general statement. □

3.5.2 Cancellation Property

An important property of the real numbers that we use all the time is the ability to cancel the same (non-zero) factor on both sides of an equation. For example if $2x = 6$ then $2x = 2 \cdot 3$ and we cancel the 2's to get $x = 3$. The reason we could "cancel" the $2's$ is simply because we could multiply both sides of the equation by the inverse of 2, namely $1/2$. That is $(1/2)(2x) = (1/2)(2 \cdot 3)$, which means $[(1/2)2]x = [(1/2)2]3$ (note the use of associativity of multiplication here), and so $x = 3$.

Luckily, this familiar property also holds for permutations.

Lemma 3.1 (Cancellation Property) *If $\alpha, \beta, \gamma \in S_n$ where $\alpha\beta = \alpha\gamma$ then $\beta = \gamma$.*

Similarly, if $\beta\alpha = \gamma\alpha$ then $\beta = \gamma$.

Proof: Multiplying both sides of $\alpha\beta = \alpha\gamma$ on the left by α^{-1} we get

$$\alpha^{-1}(\alpha\beta) = \alpha^{-1}(\alpha\gamma).$$

By associativity

$$(\alpha^{-1}\alpha)\beta = (\alpha^{-1}\alpha)\gamma.$$

and so

$$\varepsilon\beta = \varepsilon\gamma,$$

which means $\beta = \gamma$.

A similar argument shows the right cancellation property as well. □

As a consequence of the cancellation property the identity permutation is the *only* permutation that when multiplied to another permutation it leaves it unchanged. That is, it has the property that $\alpha\varepsilon = \alpha$ for any $\alpha \in S_n$. To see this, suppose β is a permutation with this property too, that is $\alpha\beta = \alpha$ for some α. Then $\alpha\beta = \alpha\varepsilon$, and by cancellation of α we have $\beta = \varepsilon$.

3.6 The Symmetric Group S_n

The set of all permutations of the set $\mathbb{Z}_n$ is called the *symmetric group of degree n*, and is denoted by S_n. in other words,

$$S_n = \{\alpha : \alpha \text{ is a permutation of } \mathbb{Z}_n\}.$$

Some authors denote the symmetric group by $\mathrm{Sym}(n)$. In these notes however, we will use S_n.

We've already seen that elements of S_n can be written in the form

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}.$$

It is straightforward to compute the cardinality of the set S_n. There are n choices for $\alpha(1)$. Once $\alpha(1)$ has been chosen, there are $n-1$ possibilities for $\alpha(2)$ (since α is injective we must have $\alpha(1) \neq \alpha(2)$). Once $\alpha(2)$ has been chosen there are $n-2$ choices for $\alpha(3)$. Continuing in this way we see that there are $n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 3 \cdot 1 = n!$ possible choices for $\alpha(1)$ to $\alpha(n)$. Each choice gives a different permutation. Therefore $|S_n| = n!$.

Let's summarize what we know so far about S_n.

- S_n, the symmetric group of degree n, is the set of all permutation of $\mathbb{Z}_n = \{1, 2, \dots, n\}$.
- $|S_n| = n!$
- Two elements $\alpha, \beta \in S_n$ can be composed (multiplied) to give another element $\alpha\beta \in S_n$.[2]
- The *identity* permutation is $\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$. It has the property that $\varepsilon\alpha = \varepsilon\alpha = \alpha$ for all $\alpha \in S_n$.
- Every $\alpha \in S_n$ has an inverse denoted by α^{-1}. The defining property of an inverse is $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$.
- $(\alpha_1\alpha_2\cdots\alpha_k)^{-1} = \alpha_k^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}$.
- Permutation composition (multiplication) is associative.
- Permutation composition (multiplication) is not necessarily commutative.
- Cancelation Property: $\alpha\beta = \alpha\gamma$ implies $\beta = \gamma$, and $\beta\alpha = \gamma\alpha$ implies $\beta = \gamma$.

3.7 Rules for Exponents

When we describe moves on Rubik's cube we write things such as: R B^2 R^{-1}. Exponents are serving two purposes here: (i) they represent inverse moves, such as R^{-1} is the inverse of R, (ii) they represent repetition of moves, such as B^2 is the move B repeated twice.

If we follow the move sequence R U^{-2} B^2 $\mathrm{R}^{-1}\mathrm{D}$ U^{-2} with the move U then the complete move sequence would be

$$\mathrm{R}\ \mathrm{U}^{-2}\ \mathrm{B}^2\ \mathrm{R}^{-1}\mathrm{D}\ \mathrm{U}^{-2}\mathrm{U}.$$

But certainly, $\mathrm{U}^{-2}\mathrm{U}$ simplifies to U^{-1}, since a counterclockwise half turn (U^{-2}) followed by a clockwise quarter turn (U) is equivalent to a counterclockwise quarter turn. This means the complete move sequence is equivalent to

$$\mathrm{R}\ \mathrm{U}^{-2}\ \mathrm{B}^2\ \mathrm{R}^{-1}\mathrm{D}\ \mathrm{U}^{-1}.$$

[2] the convention of these notes is to compose permutations from left-to-right,

We write this as (R U^{-2} B^2 R^{-1}D U^{-2}) U = R U^{-2} B^2 R^{-1}D U^{-1}.

This notation translates nicely to composition of permutations.

If $\alpha \in S_n$ and m is a positive integer then α^m denotes the product of α with itself m-times. That is, $\alpha^m = \alpha\alpha\cdots\alpha$.

We define negative exponents by the rule $\alpha^{-m} = (\alpha^{-1})^m$, where m is any positive integer.

We define the zero exponent by $\alpha^0 = \varepsilon$, where ε is the identity permutation.

An important observation is that some of the familiar "rules of exponents" apply to the composition of permutations. Specifically, for any two integers m and k and for any $\alpha \in S_n$, we have

(a) $\alpha^m\alpha^k = \alpha^{m+k}$

(b) $(\alpha^m)^k = \alpha^{mk}$

This follows precisely from the fact that we are defining an exponent to represent repeated multiplication.

One property that you may be familiar with from multiplication of real numbers is: $(ab)^m = a^m b^n$. This is *not* true for permutations: if $\alpha, \beta \in S_n$ and $m \in \mathbb{Z}$ then in general $(\alpha\beta)^m$ is not equal to $\alpha^m\beta^m$.

For real numbers this property relies on the fact that multiplication of real numbers is *commutative*. We've already seen this is not the case for permutations under composition.

However, we do have the following result.

Lemma 3.2 *If $\alpha, \beta \in S_n$ commute with each other, that is $\alpha\beta = \beta\alpha$, then for all integers m, $(\alpha\beta)^m = \alpha^m\beta^m$.*

Exercise 3.2 *Prove Lemma 3.2.*

3.8 Order of a Permutation

The **order** of a permutation $\alpha \in \mathbb{Z}_n$ is the smallest positive integer m such that $\alpha^m = \varepsilon$.

In Example 3.7 we saw that for $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ the smallest m for which $\alpha^m = \varepsilon$ is 6. We say α has *order* 6, and we write ord$(\alpha) = 6$.

As another example, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ is an element in S_3 of order 2, since $\beta \neq \varepsilon$, but $\beta^2 = \varepsilon$.

Must every permutation have a finite order? The next theorem answers this question.

Theorem 3.3 *For any $\alpha \in S_n$ there exists a positive number m for which $\alpha^m = \varepsilon$. (The smallest such m is the **order** of α, denoted ord(α).)*

Proof: Consider the set of all powers of α, $\{\alpha^k : k \in \mathbb{Z}^+\}$. Since this is a subset of the finite set S_n it must also be finite. This means all the powers of α cannot be distinct, so there must be k, ℓ such that $\alpha^k = \alpha^\ell$ where $k > \ell > 0$. Now multiplying $\alpha^{-\ell}$ to the left of both sides (i.e. cancelling α^ℓ) we get:

$$\alpha^{-\ell}\alpha^k = \alpha^{-\ell}\alpha^\ell$$

and so

$$\alpha^{k-\ell} = \varepsilon.$$

This proves the theorem. □

We can now describe precisely which integers m have the property that $\alpha^m = \varepsilon$.

Theorem 3.4 *Let α be a permutation. If $\alpha^m = \varepsilon$ then ord(α) divides m.*

Proof: Let $n = \text{ord}(\alpha)$, and suppose $\alpha^m = \varepsilon$. By the division algorithm there exist integers q and $0 \leq r < m$ such that $m = qn + r$. In other words, n goes into m q-times, with r left over. Therefore

$$\varepsilon = \alpha^m = \alpha^{qn+r} = (\alpha^n)^q \alpha^r = \varepsilon^q \alpha^r = \alpha^r.$$

Since r is smaller than the order of α this is only possible if $r = 0$. Hence n divides m. □

Exercise 3.3 *Let*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}.$$

Determine the order of (a) α (b) β (c) β^{-1} (d) γ (e) $\alpha^{-1}\gamma\alpha$.

Exercise 3.4 *Consider Rubik's cube. Determine the orders of each of the following moves by physically doing the move successively on the cube. It is best to start with your cube in the solved state so you can easily recognize when you've returned to that state.*

(a) R

(b) $R^2\, L^2\, U^2$

(c) $U^2 R$

(d) $U\, R$

If you stuck with it long enough, and didn't lose count, you would find that U R has order 105. That means you would have to apply U R a total of 105 times (or a total of 210 quarter face turns) before you get back to where you started.

One of our goals will be to thoroughly understand orders of move sequences: specifically how to compute the order of a move sequence without having to physically manipulate the cube.

For example, the move sequence R U^2 D^{-1}B D^{-1}has order 1260. We'll soon see how to compute this rather quickly by using a computer.

3.9 Exercises

1. Show that a function from a finite set A to itself is one-to-one if and only if it is onto. Is this true when A is infinite?
2. Suppose A and B are finite sets and $|A| > |B|$. Is there an *injective* function $f : A \to B$? Explain.
3. For $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, and $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ verify that $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. This provides some experimental evidence for the associative law.
4. Consider the following permutations

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 7 & 1 & 5 & 8 & 2 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 6 & 7 & 1 & 3 & 2 & 8 \end{pmatrix}.$$

   Determine each of the following.

   (a) $\alpha\beta$
   (b) $\alpha\gamma\beta$
   (c) β^{-1}
   (d) $(\gamma\beta)^{-1}$
   (e) $\beta^{-1}\gamma^{-1}$
   (f) $\alpha^{-1}\gamma\alpha$
   (g) $\text{ord}(\alpha)$
   (h) $\text{ord}(\beta)$
   (i) $\text{ord}(\alpha^{-1}\gamma\alpha)$

5. Find the inverse of each of the following permutations. Verify it is the inverse by computing the product and showing it is the identity permutation.

   (a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$
   (b) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 7 & 3 & 8 & 2 & 6 \end{pmatrix}$

6. For $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$ explain how you know $\alpha^{2011} \neq \varepsilon$, without actually computing all 2011 powers of α.
7. Show that an n-cycle $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ n & 1 & 2 & \dots & n-1 \end{pmatrix}$ has order n.
8. Show that for any $\alpha \in S_n$, $\text{ord}(\alpha) = \text{ord}(\alpha^{-1})$.
9. **There is always something that doesn't commute.** Show that if $n \geq 3$, then for every element α in S_n, if α is not the identity permutation ε, then there is some other permutation β in S_n with which α does not commute: $\alpha\beta \neq \beta\alpha$.
10. For any permutations α and β and any integer n show that $(\alpha^{-1}\beta\alpha)^n = \alpha^{-1}\beta^n\alpha$.
11. For $\alpha, \beta \in S_n$ show that if $(\alpha\beta)^2 = \alpha^2\beta^2$ then α commutes with β: that is, $\alpha\beta = \beta\alpha$.
12. Show that if $\alpha\beta\gamma\beta^{-1}\alpha = \alpha\beta\sigma\beta^{-1}\alpha$ then $\gamma = \sigma$.
    Hint: Use the cancellation property.
13. Show that the number of elements α in S_n such that $\alpha^3 = \varepsilon$ is odd. In other words, show the set $\{\alpha \in S_n \mid \alpha^3 = \varepsilon\}$ has odd cardinality.