1.4 Permutations of sets and the symmetric groups S_n

Question 1.23. There are five seats in a classroom, and five students. How many different ways are there to seat the students?

Definition 1.24. Let S be a set. A **permutation** of S is a bijective map

$$p : S \to S.$$

Example 1.25. Let $[5] = \{1, 2, 3, 4, 5\}$.
Here is an example of a permutation p of [5]:

i	1	2	3	4	5
$p(i)$	3	5	4	1	2

Notation 1.26. For any $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, \ldots, n\}$.

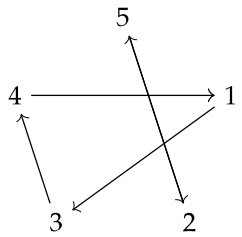
Definition 1.27. The group of *all* permutations of $[n]$ is called the **symmetric group** and is denoted S_n.

Do not confuse this with *permutation groups* in general, which are *subgroups* of symmetric groups.

Exercise 1.28. Consider our permutation $p \in S_5$ above.

(a) How does the permutation p^2 act on $[5]$?

(b) Recall that $p^2 = p \circ p$. Write down a similar chart.



To write down the **cycle notation** for a permutation, we start with an arbitrary index, such as 3, and then write down $p(3)$, and repeat until we get back to 3:

$$3 \mapsto 4 \mapsto 1 \mapsto 3$$

For p above, this gives us a 3-cycle $(3\ 4\ 1)$. Then, we choose an index that we haven't seen yet, and do the same thing: $(2\ 5)$.

If an index is fixed by a permutation, then by convention, we omit writing the 1-cycle. For example,

$$q = (12)(34) \in S_5$$

is cycle notation for the permutation given by the following chart:

i	1	2	3	4	5
$q(i)$	2	1	4	3	5

Example 1.29. There are many equivalent ways to write p in cycle notation:

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

Disjoint cycles can be written in any order, and cycles need only have their cyclic order preserved.

Exercise 1.30. Cycle notation allows us to compose permutations easily. Let

$$p = (3\ 4\ 1)(2\ 5) \qquad q = (1\ 2)(3\ 4).$$

(a) Write down p^2, p^3, and p^4 in cycle notation.
Solution: $p^2 = (3\ 1\ 4)$, $p^3 = (2\ 5)$, $p^4 = (3\ 4\ 1)$

(b) Write down qp and pq in cycle notation. (Remember, qp means $q \circ p$.)
Solution: $qp = (1\ 2)(3\ 4) \circ (3\ 4\ 1)(2\ 5) = (1\ 4\ 2\ 5)$, $pq = (3\ 4\ 1)(2\ 5) \circ (1\ 2)(3\ 4) = (1\ 5\ 2\ 3)$

We can represent permutations using **permutation matrices**. The key observation is that there is an obvious set bijection

$$[n] \cong \{e_1, e_2, \ldots, e_n\}.$$

Example 1.31. Let $\sigma = (1\ 3\ 2) \in S_3$. We can represent σ as the linear transformation that sends each $e_i \mapsto e_{\sigma(i)}$:

$$\sigma \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Definition 1.32. A **transposition** is a 2-cycle. We usually denote them by $\tau_{ij} = (i\ j)$.

Theorem 1.33. The set of all transpositions τ_{ij} (where $i \neq j$ are indices in $[n]$) generate S_n.

Proof. (Proof idea) Any permutation is a product (i.e. composition) of cycles, so One way to prove this is by exhibiting an algorithm for constructing cycles from transpositions.

For example, observe that

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2).$$

(Note once again that we first apply the transposition at the far right, and work out way left, because we are actually just composing set maps.) This reasoning works in general:

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_3)(i_1\ i_2).$$

□

Example 1.34. How can we write $p = (3\ 4\ 1)(2\ 5)$ as a composition of transpositions?

1.5 Complex numbers

The complex numbers $\mathbb{C}$ are is pervasive in mathematics and will provide us with many interesting examples of groups.

Let i be a variable satisyfing the relation $i^2 = -1$. The underlying set of $\mathbb{C}$ is $\{a + bi \mid a, b \in \mathbb{R}$. In other words, the complex numbers are just polynomials (with real coefficients) in the variable i, except that any time you see i^2, you can replace it with $-1 \in \mathbb{R}$.

This tells us how to add and multiply complex numbers. Addition is the same as vector addition in $\mathbb{R}^2$:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Multiplication is the same as for polynomials:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$

What's more interesting is that one can also divide complex numbers. That is, every nonzero complex number has a *multiplicative inverse*:

$$\frac{1}{a + bi} = (a + bi)^{-1} = \frac{1}{a^2 + b^2}(a - bi)$$

The variable of choice for complex numbers is usually z, followed by w. The **complex conjugate** of $z = a + bi$ is $\bar{z} = a - bi$.[4]

[4]This is in analogy with the conjugates we learn about in precalculus: $a \pm b\sqrt{k}$.

When we view z as a vector $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$, its length is given by $||z|| = \sqrt{a^2 + b^2}$. When we view z as a complex number, we call this the **absolute value** or **modulus** of z, and write

$$|z| = \sqrt{a^2 + b^2}.$$

Exercise 1.35. Verify that $z\bar{z} = |z|^2 = a^2 + b^2$, and observe that

$$z^{-1} = \frac{\bar{z}}{|z|^2}.$$

It is often easier to work with polar coordinates (r, θ) rather than rectangular coordinates (x, y). We can write any complex number $z = x + iy$ in polar coordinates (r, θ) where

- $r = |z|$, the length of the vector z
- θ is the angle the vector z makes with the real axis (which is identified with the x-axis in $\mathbb{R}^2$).

Recall from precalculus that to translate from (r, θ) to (x, y), we compute

$$x = r\cos\theta \qquad y = r\sin\theta.$$

For Taylor series reasons, we can write

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Euler's formula says that $e^{\pi i} = -1$, and therefore $e^{2\pi i} = 1$.

Therefore if $z = x + iy$, and (x, y) in rectangular coordinates translates to (r, θ) in polar coordinates, we can write

$$z = x + iy = re^{i\theta}.$$

We will use this notation *extensively*, because it makes complex multiplication very simple. Let $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$. Then

$$z_1 z_2 = \left(r_1 e^{i\theta_1}\right)\left(r_2 e^{i\theta_2}\right) = (r_1 r_2) e^{(\theta_1+\theta_2)i}.$$

Geometrically, multiplication by i represents rotating by $\pi/2$ counterclockwise (CCW). That is, the vector iz is just the vector z rotated by $\pi/2$.

Example 1.36. The unit circle S^1 inside $\mathbb{C}$ is the set of complex numbers of modulus 1:

$$S^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}.$$

Note that I could have also written $\theta \in [0, 2\pi)$, or any other interval of this shape of length 2π, because $e^{2\pi i} = 1$.

This is a group under complex multiplication. (See HW01 for the same group described in a different way.)

Exercise 1.37. Prove that the **circle group** S^1 (under complex multiplication) is *not* cyclic.