Now that we have looked at a bunch of abelian groups, let us look at some non abelian groups. In particular, we will be looking at an infinite familiy of non abelian groups, called permutation groups. The importance of permutation groups cannot be overstated. In a sense, every group is contained within a permutation group. This will be the content of Cayley's Theorem.

Definition 0.1 (Permutation). Let S be a set. Then a **permutation** (of S) is a bijection $\sigma : S \to S$.

We leave the reader to come with some examples of permutations.
Exercise 0.2. Let $S = \{1, 2, 3\}$. Find every permutation of S.

We have previously seen in **??** that if $S = \{1, \dots, n\}$, then the set of permutations of S forms a group under function composition. In fact, given any set A, the set of permutations on S forms a group under function composition. We denote this set with S_A.
Exercise 0.3. Let S be *any* set. Prove that the set of permutations on S forms a group under function composition.

We remark that the structure of the group S_A only depends on the cardinality of A, and not on what is in A. That is, if $|A| = |B|$ then S_A is isomorphic to S_B. We defer a proof of this to Exercise 0.20. As such when considering permutations on finite sets of size n, we only need to consider permutations on the set $\{1, \dots, n\}$.

We will focus our efforts on permutations of finite sets for now. Recall that S_n denotes the set of permutations on n things. Since the main property of an n-element set is that it contains n elements, we shall let S_n refer to the group of permutations on the set $\{1, \cdots, n\}$. To aid in our study of permutation groups, we shall introduce some notation to describe the elements of permutation groups, called *cycle notation*. To understand this notation, let us begin with an example.

Let $\sigma \in S_6$ be defined by $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 5$, $\sigma(4) = 6$, $\sigma(5) = 1$, $\sigma(6) = 2$. So, 1 goes to 3, 3 goes to 5 and 5 goes to 1. We can write this down as $(1, 3, 5)$. Additionally, 2 goes to 4 and 4 goes to 6, and 6 goes to 2. We similarly write this down as $(2, 4, 6)$. Thus, expressing σ in cycle notation, we get $\sigma = (1, 3, 5)(2, 4, 6)$.

We remark that given $\sigma \in S_n$, if $n < 10$, it is common to omit the commas in the cycle notation as there is no ambiguity about what is going on. So for instance, our σ above could be written as $(135)(246)$.

Let us see how to evaluate σ at a particular value. Suppoe that we didn't know what $\sigma(5)$ was but we do know that $\sigma = (135)(246)$. We first apply the cycle (246) to 5. Since 5 appears nowhere in this cycle, it comes out as a 5. Now we apply the cycle (135) to 5. Since 5 is at the end of the cycle, it goes to 1, so application of (135) to 5 yields 1.

$$5 \overset{(246)}{\longmapsto} 5 \overset{(135)}{\longmapsto} 1$$

Now, let $\tau = (123)$. We shall now describe how to compose the permutations σ and τ. In this case, the obvious answer is the correct one, so we have

$$\sigma\tau = \underbrace{(135)(246)}_{\sigma}\underbrace{(123)}_{\tau}.$$

As such, we compose cycles *right to left*. This agrees with how we do function composition. (The reader should be warned that some authors compose cycles left to right instead. Note that this is stupid.)

However, this form is not very helpful for determining the properties of $\sigma\tau$. It is much better if we can express $\sigma\tau$ in terms of disjoint cycles.

Definition 0.4 (Disjoint cycles). Let $\alpha = (a_1, \dots, a_n)$ and $\beta = (b_1, \dots, b_m)$. Then α and β are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

In other words, two cycles are disjoint if they share no elements in common. For example, the cycles (123) and (456) are disjoint, but the cycles (134) and (235) are not.

So to express $\sigma\tau$ in terms of disjoint cycles, we simply need to find out where all the elements go. Unfortunately, the best way to do so is to simply evaluate $\sigma\tau$ at every element. We shall do one evaluation and leave the rest for the reader to practice. Let us follow where the element 3 goes.

$$3 \overset{(123)}{\longmapsto} 1 \overset{(246)}{\longmapsto} 1 \overset{(135)}{\longmapsto} 3$$

So $\sigma(3) = 3$.

Exercise 0.5. Figure out where the rest of the elements go. Write down $\sigma\tau$ in cycle notation.

We now finish our discussion of cycle notation by remarking that cycles with only one entry are often omitted. For example, instead of writing $(1)(23)(4)(56)$, one would write $(23)(56)$ instead. Any missing element is fixed by the permutation. Of course, we have to write something down for the identity permutation, so we could say that the identity permutation is (1) or (3) or whatever.

We now begin our investigation into permutations. The following theorem justifies the preceding discussion on writing permutations as cycles. While reading the proof, the reader should keep in mind the cycle decomposition algorithm.

Theorem 0.6 (Existence of cycle decomposition)**.** Every permutation of a finite set admits a cycle decomposition. In other words, if $\sigma \in S_n$ then σ is either a cycle, or a product of disjoint cycles.

Proof. Let $S = \{1, \ldots, n\}$ let σ be a permutation on S. Pick $a_1 \in S$. Set $a_n = \sigma(a_{n-1})$, so $a_n = \sigma^{n-1}(a_1)$. This sequence is finite since all the elements are in S. Thus, there are indices i, j, where $i < j$ and $a_i = a_j$. So $a_1 = \sigma^{j-i}(a_1)$. Now set $\alpha = (a_1, \ldots, a_{j-i})$. If $S \setminus \{a_k\}_1^{j-i}$ is empty we are done. If not, pick $b_1 \in S \setminus \{a_k\}_1^{j-i}$ and repeat the same procedure. Let β be the cycle formed from doing this. We now prove that β and α are disjoint cycles (the general case follows easily). Suppose not. Say x shows up in both α and β. If $x = \beta^k(b_1) = \alpha^m(a_1)$, then this means that $x = \sigma^k(b_1) = \sigma^m(a_1)$, but then we would have $\sigma^{m-k}(a_1) = b_1$, so b_1 shows up in the sequence (a_n). But this contradicts $b_1 \in S \setminus (a_n)$. □

The astute reader may have already noticed the following fact: If α, β are disjoint cycles then the order in which they are evaluated does not matter.

Theorem 0.7 (Disjoint cycles commute)**.** If α and β are disjoint cycles, then $\alpha\beta = \beta\alpha$.

Proof. We shall not rob the reader of the joy of discovering the proof of this theorem on their own. □

Exercise 0.8. Prove Theorem 0.7.

Disjoint cycles have yet another advantage up their sleeve: we are able to quickly determine their order.

Theorem 0.9 (Order of 2 disjoint cycles is lcm of their length)**.** Suppose α and β are disjoint cycles of length m and n respectively. Then,

$$|\alpha\beta| = \operatorname{lcm}(|\alpha|, |\beta|).$$

Proof. Since n, m are the orders of α, β respectively, we let $l = \operatorname{lcm}(n, m)$. Then, $(\alpha\beta)^l = \alpha^l\beta^l = e$ by Theorem 0.7, so $|\alpha\beta| \leq l$. If $k \leq l$ and k is the order of $\alpha\beta$ then we have n and m both dividing k, so k is a common multiple of n and m. Thus $k = l$. □

Exercise 0.10. Prove that if α is a cycle of length n, then $|\alpha| = n$.

Exercise 0.11. Generalize Theorem 0.9.

Given a permutation, we would like to write it as a product of 2-cycles. It is always possible to do so.

Proposition 0.12 (Existence of 2-cycle decomposition)**.** *If σ is a permutation on the set $\{1, \ldots, n\}$ then σ can be decomposed as the product of 2-cycles.*

Proof. Suppose σ is a cycle. Let $\sigma = (a_1, \ldots, a_k)$. Then direct computation shows that

$$\sigma = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1 a_2).$$

The proof of the general case can be easily obtained by using Theorem 0.6. □

Definition 0.13 (Even/Odd Permutation)**.** Let σ be a permutation on a finite set. Then, σ is **even** if it admits a 2-cycle decomposition into an even number of 2-cycles.

An odd permutation is defined similarly. We call the oddness or evenness of a permutation its *parity*.

One may be wondering whether a 2-cycle decomposition is unique. Unfortunately, this is not true.
Example 0.14 (Non-uniqueness of 2-cycle decomposition)**.**

$$(12345) = (54)(53)(52)(51)$$
$$(12345) = (54)(52)(21)(25)(23)(13).$$

//

Can a permutation be both even or odd? No. In fact, if a permutation can be decomposed as an even number of 2 cycles, then any 2-cycle decomposition of this permutation must also result in an even number of 2 cycles.

Let us first find out the parity of the identity permutation. Since $e = (12)(12)$ it makes sense that it should be even.
Proposition 0.15 (Identity permutation is even)**.** *Let e be the identity permutation. If $e = \alpha_1 \cdots \alpha_n$ where α_i is a 2-cycle, then n is even.*

Proof. Painful. **TODO: Insert proof** □

Theorem 0.16 (Parity of a permutation is well-defined)**.** If σ is a permutation (on a finite set), then it is either even or odd.

Proof. Let $\sigma = \alpha_1 \cdots \alpha_k$ $\sigma = \gamma_1 \cdots \gamma_m$ be 2-cycle decompositions of σ. Then, keeping in mind a 2-cycle is its own inverse,

$$e = \sigma\sigma^{-1} = (\alpha_1 \cdots \alpha_k)(\gamma_m \cdots \gamma_1).$$

So Proposition 0.15 this implies $k + m$ is even. So k, m are both odd or both even. □

The set of even permutations of a permutation group is extremely important, and so it deserves its own name. Although we will not see its importance at the moment[1], it is worth introducing it at this point.

Definition 0.17 (Alternating group)**.** Let A_n denote the set of even permutations of S_n.

You probably already suspect that A_n is a group now.
Exercise 0.18. Prove that A_n is a subgroup of S_n.

You might be thinking to yourself that there should be as many even permutations as odd permutations. This is indeed true. If $n > 1$, then A_n has order $n!/2$.
Exercise 0.19. Prove that $|A_n| = n!/2$ when $n > 1$.

Hint: If α is even, then $(12)\alpha$ is odd. Additionally, if $\alpha \neq \beta$ then $(12)\alpha \neq (12)\beta$.

0.1 Group actions

To be done

[1] The alternating group has no nontrivial proper normal subgroups. You might have seen this called a *simple group*. There is a rather famous theorem that classifies all the finite simple groups. The alternating groups form an infinite family of finite simple groups.

0.2 Problems

Exercise 0.20 (Structure of permutation group)**.** Recall that the cardinality of a set A is equal to the cardinality of a set B if there exists a bijection from A to B. Let A, B be sets and suppose that the cardinality of A equals to the cardinality of B. Thus we may let $\gamma : A \to B$ be a bijection. Show that S_A is isomorphic to S_B.

Hint: Think about how a permutation of A can be changed into a permutation of B, and conversely.

Exercise 0.21. Suppose H is a subgroup of S_n and H has odd order. Prove that H is a subgroup of A_n.

Exercise 0.22. Prove that if σ is a permutation with odd order, then σ is even.

Exercise 0.23. Show that if $n \geq 3$, then $Z_(S_n)$ is trivial.

Exercise 0.24. Let $\alpha \in S_n$. Without using Lagrange's theorem, prove that the order of α divides S_n.