0.1 Permutations and cycles

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, or $\mathrm{Sym}(A)$, to avoid things like S_S (which is confusing). This is called the *group of symemtries on the set* A. Of course, when n is a positive integer, we also have S_n, the group of symmetries on n things[1].
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 0.28. 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.

[1] Actually, it turns out that natural numbers are sets, since they are ordinals. So the notation S_n and S_A is not abusive. But if you don't know about this fact, then it is abusive notation.

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)**.**

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

A simpler example would be $(123) = (13)(12) = (12)(23) = (23)(13)$. //

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. It turns out that this is true. Unfortunately, the following proof is very long and painful.

Alternative proofs of the fact that the parity of permutation is well-defined can be found in Exercise 0.33 or Exercise 0.34.

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. Suppose otherwise. Say $\beta_1 \cdots \beta_n = e$ where n is odd. Note that $n > 1$. Without loss of generality assume $\beta_1 = (ab)$. Then there is some 2-cycle β_i, $i > 1$, which contains a, otherwise this product will send a to b.

We make a few additional assumptions, which can be done without loss of generality:

1. Assume that i is the smallest such index which contains a;
2. assume that this product is one with the fewest number of a's as a entry in any cycle.

If $i = 2$, then $\beta_1\beta_2$ is $(ab)(ab)$ or $(ab)(ac)$ where $c \neq b$. (Note that if it is of the form $(ab)(ca)$ then we have $(ca) = (ac)$ anyway.) In the first case, $(ab)(ab)$ is the identity, so we now have the identity being a product of an odd number of 2-cycles, with fewer appearances of a's, contradicting assumption 2. In the latter, we have $(ab)(ac) = (ac)(bc)$. We may replace $\beta_1\beta_2$ with $\beta_1'\beta_2' = (ab)(bc)$ in our product. This contradicts assumption 2 again. Since $i = 2$ gives us contradictions, let's assume $i > 2$. Now, β_{i-1} does not contain a, by assumption 1, but it has to contain c. If this is not true, β_i and β_{i-1} are disjoint. We now see that □

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[2], 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 $(12)\alpha \neq (12)\beta$.

0.2 Group actions

We open the discussion about group actions with a motivating example. Let $G = \{ r^0, r^1, r^2, r^3 \}$ where r is rotation clockwise by 90 degrees. Consider the diagram of the square, and follow where the dot goes.

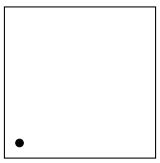

Figure 1: Helpful square to visualize rotation group acting on square.

In some sense, the group of rotations is acting on the square, changing its position. We can perhaps envision a rotation as some kind of function on the square. Let S represent the square. Imagine labelling each of the edges of the square by 1,2,3,4. So we can think of rotating the square by 90 degrees as $r(S)$, whatever that means. Now, if we do $r(r(S))$, that is rotating by 180 degrees. But if we do $r^2(S)$, it is also rotating by 180 degrees. In the former, we apply the rotation action and then the rotation action, but in the latter, we multiply r with itself in the group G and then apply the action of the result on S. Naturally, it should make sense that these notions agree. Now, let's take a look at how the identity rotation acts on the square. Notice that the rotation by 0 degrees fixes every edge of the square.

As another example, let us consider a tuple (1,2,3). We can rearrange the components in the tuple, to be something like (2,1,3) or like (3,2,1). Now, we know that the act of rearranging something is simply a permutation. In this example, if σ is the permutation that sends 1 to 2, 2 to 1 and 3 to itself, then $(\sigma(1), \sigma(2), \sigma(3)) = (2, 1, 3)$. It's not too hard to figure out how to extend this idea to any other $\sigma \in S_3$.

Definition 0.20 (Group action). Let G be a group and S a set. Then a **action of G on S** is a function $f : G \times S \to S$ such that:

1. **(Associativity)** For all $g, h \in G$ and $s \in S$, $f(gh, s) = f(g, f(h, s))$.
2. **(Identity)** For all $s \in S$, $f(e, s) = s$.

As you can see above, writing $f(g, s)$ gets annoying very fast. Thus, whenever the group action is clear, we shall use $g \cdot s$, to mean $f(g, s)$. When there is no danger of confusing the group action with group multiplication, we shall write gs instead.

We shall now see some examples of group actions.
Example 0.21 (Symmetric group)**.** Let $S = \{ 1, \ldots, n \}$ and let $G = S_n$. Then we can define an action of G on S by declaring $\sigma \cdot s := \sigma(s)$. //
Example 0.22. Let $S = \mathbb{R}$ be the real numbers, and let $G = \mathbb{Z}$. We can define an action of G on S by declaring $n \cdot r = n + r$. //

[2]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.

Example 0.23 (Group acting on itself)**.** Let G be a group. Now, if we momentarily forget that G is a group, G is also a set. Thus, we can define a very natural group action on G by $g \cdot h := gh$. So G acts on G by left multiplication. //

Definition 0.24 (Orbit)**.** Let G act on S. For $s \in S$, we define the **orbit of** s to be

$$\mathrm{Orb}_G(s) = \{\, g \cdot s : g \in G \,\}.$$

So the orbit is the image of G under the function $g \mapsto f(g, s)$.

Definition 0.25 (Stabilizer)**.** Let G act on S. For $s \in S$, we define the **stabilizer of** s to be

$$\mathrm{Stab}_G(s) = \{\, g \in G : g \cdot s = s \,\}.$$

So the stabilizer of s is the set of all $g \in G$ that fixes s under the group action. Of course, a natural question is whether the stabilizer is a subgroup. The following exercise answers that question.
Exercise 0.26. Prove that the stabilizer of s is a subgroup.

A burning question at this point might be the following: Aren't group actions kind of just like permutations? Indeed, this is an excellent question, as we have put in the chapter on permutation groups. Suppose G acts on X. Let us fix a $g \in G$. Consider the function $f : X \to X$ given by $x \mapsto g \cdot x$. It turns out that f is a bijection, and thus f is a permutation of X. Now, let us call σ_g the function that applies the action of g on X, i.e. $\sigma_g(x) = g \cdot x$. It seems that we can construct a map from G into S_X. Of course, this map would be $g \mapsto \sigma_g$. Since we are studying group theory, it is natural to wonder whether this is a homomorphism. Indeed, it is. See Exercise 0.35.

Our study of permutation groups takes a temporary hiatus with the following theorem. If it seems trivial to you, it's due to the power of excellent definitions. This shows us the power of group actions and once again reminds us the importance of constructing good definitions.

Theorem 0.27 (Cayley's Theorem)**.** Every group is isomorphic to a group of permutations.

Proof. See Exercise 0.36. □

0.3 Problems

Exercise 0.28 (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 0.29. Suppose H is a subgroup of S_n and H has odd order. Prove that H is a subgroup of A_n.
Exercise 0.30. Prove that if σ is a permutation with odd order, then σ is even.
Exercise 0.31. Show that if $n \geq 3$, then $Z(S_n)$ is trivial.
Exercise 0.32. Let $\alpha \in S_n$. Without using Lagrange's theorem, prove that the order of α divides S_n.
Exercise 0.33 (An alternative proof that the sign of a permutation is well-defined)**.** We give an alternative proof that the sign of a permutation is well-defined, due to [Jac09, p. 50].

Recall that an n-cycle can be decomposed into $n-1$ transpositions. If γ is an n-cycle, let $\tilde{N}(\gamma) = n - 1$, the number of transpositions that γ is a product of. Given some $\alpha \in S_n$, let

$$\alpha = \gamma_1 \cdots \gamma_n,$$

be the disjoint cycle decomposition of α. Now we can define $N(\alpha) = \sum_{i=1}^{n} \tilde{N}(\gamma_i)$.

More concretely, if γ_i is a u_i cycle, then $N(\alpha) = \sum_{i=1}^{n} u_i - 1$. Also note that $N(e) = 0$.

(a) Show that $N(\alpha)$ is uniquely determined by α.

(b) Let $a, b, c_1, \ldots, c_h, d_1, \ldots, d_k$ be distinct elements, where $h, k \geq 0$. Verify that

$$(ab)(ac_1 \cdots c_h b d_1 \cdots d_k) = (bd_1 \cdots d_k)(ac_1 \cdots c_h).$$

(c) Let $p = (ac_1 \cdots c_h b d_1 \cdots d_k)$. Check that $N(p) = h + k + 1$, and that $N((ab)p) = h + k$.

(d) Let α be some permutation. Show that $N((ab)\alpha) = N(\alpha) - 1$ if a, b occur in the same cycle in the decomposition of α into disjoint cycles, and $N((ab)\alpha) = N(\alpha) + 1$ if a, b occur in different cycles.

(e) Suppose that α is a product of m transpositions. Prove that $N(\alpha) = \sum_{i=1}^{m} \varepsilon_i$, where $\varepsilon_i = \pm 1$. *Hint: Decompose α into disjoint cycles first to make life easy.*

(f) Prove that $N(\alpha)$ and m have the same parity, i.e. $N(\alpha)$ is even if and only if m is even.

Exercise 0.34 (Another proof that the sign of a permutation is well-defined)**.** Let T be the set of all polynomials in $x_1, \ldots, x_n$. For $\sigma \in S_n$, define a group action on T by $\sigma \cdot x_i = x_{\sigma(i)}$ and extending this in a natural way, so for instance, we have $\sigma \cdot (4x_i + 3x_i x_j) = 4x_{\sigma(i)} + 3x_{\sigma(i)} x_{\sigma(j)}$. Let $\Delta = \prod_{i>j}(x_i - x_j)$, where i, j runs from 1 to n.

1. Prove that the group action defined is actually a group action.
2. Show that if τ is a transposition, $\tau \cdot \Delta = -\Delta$.
3. Prove that if σ can be decomposed into an even number of transpositions, then any decomposition of σ into transpositions yields an even number of permutations.

Exercise 0.35 (Group actions and the symmetric group)**.** Let G act on X. For a fixed $g \in G$, define $\sigma_g(x) = g \cdot x$.

1. For every $g \in G$, show that σ_g is a bijection.
2. Show that the map $g \mapsto \sigma_g$ is a homomorphism. (i.e. $\sigma_g \sigma_h = \sigma_{gh}$)

Exercise 0.36 (Cayley's Theorem)**.** Prove Cayley's Theorem.

Exercise 0.37 (Orbits partition a set)**.** Let G be a group acting on a set S. Define $\sim$ on S by

$$x \sim y \iff x \in \mathrm{orb}_G(y).$$

Show that $\sim$ is an equivalence relation, and that the equivalence class of x under $\sim$, $[x]_\sim$ is precisely $\mathrm{orb}_G(x)$.