1 Permutations

Definition 1. A permutation on X where X is a set, is a bijective function $f : X \mapsto X$.

We will only be dealing with permutations for finite sets because they give us very useful properties.

Definition 2. Let $X = \{1, 2, 3, \ldots, n\}$. Then, the set of bijective functions on X is a group called S_n, the symmetric group on n letters.

Theorem 1. $\#S_n = n!$.

Hopefully this is not too hard to see.

Definition 3. Let $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ be distinct elements. An $k-$cycle is a permutation $\sigma \in S_n$ such that $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $a_3 \mapsto a_4 \ldots a_k \mapsto a_1$ and for all $x \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_k\}$, $\sigma(x) = x$. We write $\sigma = (a_1 a_2 \ldots a_k)$. Let τ be a cycle $(b_1 b_2 \ldots b_\ell)$. We say the length of τ is $\#\{b_1, b_2, \ldots, b_\ell\}$. We say σ, τ are disjoint if the sets $\{a_1, a_n \ldots, a_k\}$ and $\{b_1, b_2, \ldots, b_\ell\}$ are disjoint.

A cycle basically shifts every element in the set $\{a_1, a_2, a_3, \ldots, a_k\}$ by some amount. Some immediate observations are that the group generated by a $k-$cycle has order k. Furthermore, disjoint cycles also commute with each other, i.e. if σ, τ are disjoint then $\sigma\tau = \tau\sigma$. We can also prove the following:

Theorem 2. Let $\sigma \in S_n$. Then, σ can be written uniquely as a product of disjoint cycles up to order.

Proof. We prove this constructively by giving an explicit method to decompose σ into disjoint cycles. Let $\sigma \in S_n$ so σ permutes $\Lambda = \{a_1, a_2, \ldots, a_k\}$ where the elements in $\Lambda = \{a_1, a_2, \ldots, a_k\}$ are ordered such that $a_1 < a_2 < \ldots < a_k$ based on the ordering in $\mathbb{N}$. By construction, every fixed element is not in $\Lambda = \{a_1, a_2, \ldots, a_k\}$. Pick $a_{\Lambda_1} = a_1$, and then consider $\sigma(a_{\Lambda_1}), \sigma^2(a_{\Lambda_1}), \ldots, \sigma^{r_{\Lambda_1}}(a_{\Lambda_1})$ such that $r_{\Lambda_1} + 1$ is the smallest natural number where $\sigma^{r_{\Lambda_1}+1}(a_{\Lambda_1}) = a_{\Lambda_1}$, and put them into the set $\Lambda_1 = \{a_{\Lambda_1}, \sigma(a_{\Lambda_1}), \ldots \sigma^{r_{\Lambda_1}}(a_{\Lambda_1})\}$. Now consider the smallest a_i that is not in the previous Λ_j and consider $\sigma(a_{\Lambda_2}), \sigma^2(a_{\Lambda_2}), \ldots, \sigma^{r_{\Lambda_2}}(a_{\Lambda_2})$ such that $r_{\Lambda_2} + 1$ is the smallest natural number where $\sigma^{r_{\Lambda_2}+1}(a_{\Lambda_2}) = a_{\Lambda_2}$, and put them into the set $\Lambda_2 = \{a_{\Lambda_2}, \sigma(a_{\Lambda_2}), \ldots \sigma^{r_{\Lambda_2}}(a_{\Lambda_2})\}$. Repeat until every a_i belongs in some Λ_j. This process must terminate since σ can only permute a finite number of elements, and we have that $\Lambda_1, \Lambda_2, \ldots, \Lambda_k$ partitions Λ. Then, by construction, it is clear that $\sigma = (a_{\Lambda_1} \sigma(a_{\Lambda_1}) \ldots \sigma^{r_{\Lambda_1}}(a_{\Lambda_1}))(a_{\Lambda_2} \ldots \sigma^{r_{\Lambda_2}}(a_{\Lambda_2})) \ldots (a_{\Lambda_k} \ldots \sigma^{r_{\Lambda_k}}(a_{\Lambda_k}))$ since σ permutes every $a_i \in \Lambda_j$ cyclically by construction of Λ_j, so it remains to show uniqueness. Let every cycle $(a_{\Lambda_i} \sigma(a_{\Lambda_i}) \ldots \sigma^{r_{\Lambda_i}}(a_{\Lambda_i}))$ be denoted as ρ_i. For uniqueness, suppose $\sigma = \tau_1 \tau_2 \ldots \tau_d$ where every τ is a disjoint cycle. By construction of the Λ_i, $d \geq k$. Pick τ_i to be the cycle that permutes a_1. The cycle length must be $r_{\Lambda_1} + 1$ by minimality of $r_{\Lambda_1} + 1$, and furthermore, $\sigma^i(a_1)$ is permuted by τ_i, and it must be in the same manner as ρ_1 by construction. Repeat with every $a_{\Lambda_i} \in \Lambda_i$ and get that every ρ_i must correspond to some τ_j. This however exhausts every element permuted by σ so there cannot be any remaining τ_i that permute other elements. Hence, $d = k$ and since every τ_j is in one-to-one correspondence with some ρ_i and thus σ has a unique decomposition up to order. □

2 Transpositions and the Alternating Group

Cycle decomposition turns out to be pretty useful in general, but for our purposes, we will use it as a lemma to prove another theorem.

Definition 4. A transposition is a 2-cycle.

Theorem 3. Every $\sigma \in S_n$ for $n \geq 2$ can be decomposed into a product of transpositions.

Note that this decomposition does not have to be unique.

Proof. By Theorem 2, it suffices to check that every cycle can be decomposed into a product of transpositions. We proceed with induction on the length of a cycle. Let $\tau = (a_1 a_2 \dots a_k)$.

- If τ has length 1, then $\tau = (12)(21)$ so we are done.
- Suppose this holds for any cycle with length ¡ 1. Then, τ has length 2 or more.
  - If τ has length 2, we are done.
  - Otherwise, $\tau = (a_1 a_2)(a_2 a_3 \dots a_k)$ and $(a_2 a_3 \dots a_k)$ has length ¡ k so we are done.

By induction we have our result. □

Transpositions are useful because of the following theorem:

Theorem 4. Let $\sigma \in S_n$. Then,

- If σ can be decomposed into a product of even number of transpositions, it can only be decomposed into a product of even number of transpositions.
- If σ can be decomposed into a product of odd number of transpositions, it can only be decomposed into a product of odd number of transpositions.

There are several ways of proving this, one way would be by induction to show that this is true for e and then for cycles, another clever proof is in Jacobson, and finally this proof is taken and adapted from a later part of Jacobson in an exercise.

Proof. Define $\Delta = \prod_{i>j}(x_i - x_j)$ where x_i is an indeterminate over $\mathbb{Z}$ and suppose there are n indeterminates. Let τ be a transposition. Then, τ fixes all the terms in $\prod_{i>j}(x_i - x_j)$ except for some k, ℓ in which $(x_k - x_\ell)$ becomes $(x_\ell - x_k) = -(x_k - x_\ell)$ ($(x_i - x_k)$ and $(x_i - x_\ell)$ will just swap and same for other terms containing x_k, x_ℓ apart from $(x_k - x_\ell)$) so $\Delta \to -\Delta$ under τ. Let π be a product of an even number of transpositions. Then, we know $\Delta \to \Delta$ under π but π being factorized into an odd number of transpositions will give $\Delta \to -\Delta$ instead, a contradiction. Hence, π can only be factored into a product of an even number of transpositions. □

Definition 5. The sign of a permutation σ, denoted $\text{sgn}(\sigma)$, is 1 if σ can be factored into a product of even number of transpositions and -1 if σ can be factored into a product of odd number of transpositions. If $\text{sgn}(\sigma) = 1$ we say σ is an even permutation and if $\text{sgn}(\sigma) = -1$ we say σ is an odd permutation.

Proposition 1. The set of even permutations is a subgroup of S_n.

Proof. Let σ, τ be even permutations. $\tau^{-1}\tau = e$ and e, τ are even so τ^{-1} is even as well. Hence, $\sigma\tau^{-1}$ is even and by the subgroup test the result follows. □

Definition 6. We call the subgroup of even permutations of S_n the alternating group A_n.

Proposition 2. A_n has index 2.

Proof. There are only two cosets of A_n, namely the even permutations and the odd permutations, so the result follows. □

The above result also tells us that exactly half of S_n are even permutations, and the other half are odd.

3 Conjugacy classes of S_n

Definition 7. Let G be a group and $x \in G$. Then, the conjugacy class of x is $\mathrm{Cl}(x) = \{yxy^{-1} | y \in G\}$.

Proposition 3. Let $\sigma, \tau \in S_n$. Then, $\sigma\tau\sigma^{-1} = \tau(\sigma(1), \sigma(2) \ldots, \sigma(n))$.

Proof. τ can be decomposed into a product of disjoint cycles and disjoint cycles commute. Hence, it suffices to show $\sigma(i_1 i_2 \ldots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))$. This is equivalent to proving $\sigma(i_1 i_2 \ldots i_r) = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))\sigma$ since multiplying both sides by σ^{-1} will yield $\sigma(i_1 i_2 \ldots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))$. We check $\sigma(i_1 i_2 \ldots i_r)(i_k) = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))\sigma(i_k)$ for an arbitrary i_k. For the LHS, notice

$$\sigma(i_1 i_2 \ldots i_r)(i_k) = \sigma(i_{k+1})$$

And note that if $k = r$, then $i_{k+1} = i_1$. Now for the RHS, notice

$$\begin{aligned}(\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))\sigma(i_k) &= (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))(\sigma(i_k)) \\ &= \sigma(i_{k+1})\end{aligned}$$

where if $k = r$, then $i_{k+1} = i_1$. Hence, LHS = RHS and $\sigma(i_1 i_2 \ldots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r))$ as required. □

Corollary 1. Suppose $\sigma = \tau_1\tau_2\ldots\tau_d \in S_n$ where each τ_i is a cycle of length α_i and they are all disjoint. Then, the conjugacy class of σ is the set of all elements $\rho_1\rho_2\ldots\rho_d$ where each ρ_i has length α_i and they are all disjoint.

The proof follows directly from the above proposition.

4 Exercises

These are exercises which will be worked through in the reading group. You are more than welcome to try them beforehand, but you are not expected to. Solutions will be posted after the reading section.

1. Show that for $n \geq 3$, every $\sigma \in A_n$ can be written as a product of $3-$cycles.
2. Show that S_n is generated by $(1n), (1\ n-1), \ldots, (12)$
3. Show that S_n is generated by $(12)(23)(34)\ldots(n-1\ n)$
4.
   - Consider S_9. Show that $H = \langle (123), (456), (789) \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
   - Find a group of order 81 in S_9. (Hint: Come up with a good choice of $\sigma \in S_n$ such that $\sigma H \sigma^{-1} = H$ and $\sigma \notin H$)
5. Give a formula for counting the number of distinct conjugacy classes in S_n.