3 Symmetric groups (09/25)

Lemma 3.1. *Let X be a set. Let S_X be the set of bijections $f\colon X \to X$. On S_X we define a binary operation via $f \circ g$, the composition of f and g. This makes S_X into a group.*

Proof. Let $\mathrm{id}_X\colon X \to X$ be the function $\mathrm{id}_X(x) = x$ for all $x \in X$. This is an identity element for S_X. Indeed, if $f\colon X \to X$ is another function, then $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x) = \mathrm{id}_X(f(x)) = (\mathrm{id}_X \circ f)(x)$ for all $x \in X$, so $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$.[1] Associativity follows from the fact that $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)$. Finally, the existence of inverses follows because each $f \in S_X$ is a bijection; the inverse of f is the inverse function f^{-1}. □

Definition 3.2. The group S_X is called the **group of permutations of** X. When $X = \{1, \dots, n\}$, we write S_n for S_X. This is called the **permutation group on** n **symbols** or the **symmetric group of degree** n. We write e for the identity element of S_n.

Lemma 3.3. *The symmetric group S_n on degree n has $n! = n(n-1)(n-2)\cdots 1$ elements for $n \geqslant 1$.*[2]

Proof. We prove the result by induction. Let s_n be the number of bijections from a set with n elements to another set with n elements. We want to show $s_n = n!$. When $n = 1$, this is true because there is exactly 1 function from a set with 1 element to another set with 1 element. Now, suppose the result is true for $1, \dots, n-1$. In particular, $s_{n-1} = (n-1)!$. To specify a bijection $f\colon \{1, \dots, n\} \to \{1, \dots, n\}$, we must choose $f(1)$. Let $Y = \{1, \dots, n\} - \{f(1)\}$. Then, the rest of the values of f are determined by a bijective function $f'\colon \{2, \dots, n\} \to Y$. There are n choices of $f(1)$ and for each such choice $s_{n-1} = (n-1)!$ for f'. Thus, there are $n \cdot (n-1)! = n!$ bijections f, so $s_n = n!$, as desired. □

Definition 3.4. Fix $n \geqslant 1$ and consider the symmetric group S_n of degree n. A **cycle** of order k is an ordered string $(a_1\, a_2\, \cdots\, a_k)$ where $a_1, \dots, a_k \in \{1, \dots, n\}$ are distinct. We view a cycle as a bijection $\sigma = (a_1\, \cdots\, a_k)\colon \{1, \dots, n\} \to \{1, \dots, n\}$, and hence as an element of S_n, by letting

$$\sigma(x) = \begin{cases} a_{k+1} & \text{if } x = a_1, \dots, a_{k-1}, \\ a_1 & \text{if } x = a_k, \text{ and} \\ x & \text{otherwise.} \end{cases}$$

In words, $\sigma = (a_1\, \cdots\, a_k)$ is the function which takes a_1 to a_2, a_2 to a_3 and so on, all the way to a_k to a_1. It does not change other elements.

Example 3.5. If $i \in \{1, \dots, n\}$, then the cycle (i) of length 1 is equal to the identity element of S_n.

Example 3.6. Recall that if G is a group and $a \in G$, then **the order of** a, if it exists, is the least integer $k \geqslant 1$ such that $a^k = e$. Write $|a| = k$ for the order of a. (Written additively, this would be the least $n \geqslant 1$ such that $na = 0$.) If $f = (a_1\, \cdots\, a_k)$ is a cycle, then its order is k.

Definition 3.7. A **transposition** is a cycle $(a\, b)$ of length 2. If $f = (a\, b)$, then $f^2 = e$, so $f^{-1} = f$.

Proposition 3.8. *If X is a set with at least 3 elements, then S_X is not abelian. In particular, if $n \geqslant 3$ be an integer, then S_n is not abelian.*

[1] We use throughout that two functions f and g from X to Y are equal if and only if $f(x) = g(x)$ for all $x \in X$.

[2] It also makes sense to write S_0 for $S_\emptyset$; this group has 1 element.

Proof. We can assume that X contains the set $\{1, 2, 3\}$. We compute the compositions

$$(1\,2) \circ (2\,3) = (1\,2\,3) \quad \text{and} \quad (2\,3) \circ (1\,2) = (1\,3\,2).$$

These cycles represent different functions on $\{1, \ldots, n\}$, so $(1\,2) \circ (2\,3) \neq (2\,3) \circ (1\,2)$. (Here, as in Definition 3.4, the cycles given act as the identity away from $\{1, 2, 3\}$.) □

Remark 3.9. Note that as an element of S_n there is no difference between $(a_1\, a_2\, \cdots\, a_n)$ and $(a_2\, a_3\, \cdots\, a_n\, a_1)$. But, as in the previous proof, if two cycles $(a_1\, \cdots\, a_k)$ and $(b_1\, \cdots\, b_m)$ start with the same element $a_1 = b_1$, then they are the same if and only if $m = k$ and $b_i = a_i$ for $1 \leqslant i \leqslant k$.

Lemma 3.10 (Disjoint cycles commute)**.** *Suppose that $f = (a_1\, \cdots\, a_k)$ and $g = (b_1\, \cdots\, b_m)$ are disjoint cycles, meaning that $a_i \neq b_j$ for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant m$. Then, $f \circ g = g \circ f$.*

Proof. Fix $x \in \{1, \cdots, n\}$. If x is not in $\{a_1, \ldots, a_k\}$, then $f(x) = x$ and $g(x)$ is also not in $\{a_1, \ldots, a_k\}$ so that $(f \circ g)(x) = f(g(x)) = g(x) = g(f(x)) = (g \circ f)(x)$. The same holds if x is not in $\{b_1, \ldots, b_m\}$. But, the union of the complements of $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_m\}$ is all of $\{1, \ldots, n\}$. So, $f \circ g$ and $g \circ f$ are equal on all of $\{1, \ldots, n\}$ and hence are equal. □

Notation 3.11. Since disjoint cycles commute, if $(a_1\, \cdots\, a_k)$ and $(b_1\, \cdots\, b_m)$ are disjoint cycles, we write $(a_1\, \cdots\, a_k)(b_1\, \cdots\, b_m)$ for their composition, in any order. Thus, for example, $(1\,2)(3\,4) = (1\,2) \circ (3\,4) = (3\,4) \circ (1\,2)$. We also make this convention for compositions of multiple pairwise disjoint cycles.

3.1 Exercises

Exercise 3.1. Let $f = (a_1\, \cdots\, a_k)$ be a cycle of length k in S_n. Write the inverse of f as a cycle.

Exercise 3.2. Let $f = (a_1\, \cdots\, a_k)$ be a cycle of length k in S_n. Prove that f has order k.

Exercise 3.3. Let $f = (a_1\, \cdots\, a_k)$ be a cycle of length k in S_n. Fix $s \geqslant 1$. Find (and prove) necessary and sufficient conditions for f^s to be a cycle. Hint: first consider the case of $s = 2$.

Exercise 3.4. Let $\mathbf{Z}/N = \{0, \ldots, N-1\}$. Equip $\mathbf{Z}/N$ with the binary operation given by multiplication modulo N, so that if $a, b \in \mathbf{Z}/N$, then $a \cdot_N b = r$ where $ab = qN + r$ where $r \in \{0, \cdots, N-1\}$. We write $ab \equiv r \mod N$.

(a) Show that this binary operation makes $\mathbf{Z}/N$ into a commutative monoid with identity element 1.

Let $(\mathbf{Z}/N)^\times \subseteq \mathbf{Z}/N$ be the subset of elements $a \in \mathbf{Z}/N$ such that there exists $b \in \mathbf{Z}/N$ with $ab \equiv ba \equiv 1 \mod N$.

(b) Show that $(\mathbf{Z}/N)^\times$ is an abelian group.

(c) Show that $(\mathbf{Z}/N)^\times$ consists of the elements of $\mathbf{Z}/N$ which are relatively prime to N.