EXERCISES

1. Let σ be the permutation

$$1 \mapsto 3 \qquad 2 \mapsto 4 \qquad 3 \mapsto 5 \qquad 4 \mapsto 2 \qquad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \qquad 2 \mapsto 3 \qquad 3 \mapsto 2 \qquad 4 \mapsto 4 \qquad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

2. Let σ be the permutation

$1 \mapsto 13$	$2 \mapsto 2$	$3 \mapsto 15$	$4 \mapsto 14$	$5 \mapsto 10$
$6 \mapsto 6$	$7 \mapsto 12$	$8 \mapsto 3$	$9 \mapsto 4$	$10 \mapsto 1$
$11 \mapsto 7$	$12 \mapsto 9$	$13 \mapsto 5$	$14 \mapsto 11$	$15 \mapsto 8$

and let τ be the permutation

$1 \mapsto 14$	$2 \mapsto 9$	$3 \mapsto 10$	$4 \mapsto 2$	$5 \mapsto 12$
$6 \mapsto 6$	$7 \mapsto 5$	$8 \mapsto 11$	$9 \mapsto 15$	$10 \mapsto 3$
$11 \mapsto 8$	$12 \mapsto 7$	$13 \mapsto 4$	$14 \mapsto 1$	$15 \mapsto 13.$

Find the cycle decompositions of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

3. For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order.
4. Compute the order of each of the elements in the following groups: **(a)** S_3 **(b)** S_4.
5. Find the order of $(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$.
6. Write out the cycle decomposition of each element of order 4 in S_4.
7. Write out the cycle decomposition of each element of order 2 in S_4.
8. Prove that if $\Omega = \{1, 2, 3, \ldots\}$ then S_Ω is an infinite group (do not say $\infty! = \infty$).
9. **(a)** Let σ be the 12-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For which positive integers i is σ^i also a 12-cycle?
   (b) Let τ be the 8-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$. For which positive integers i is τ^i also an 8-cycle?
   (c) Let ω be the 14-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$. For which positive integers i is ω^i also a 14-cycle?
10. Prove that if σ is the m-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $|\sigma| = m$.
11. Let σ be the m-cycle $(1\ 2\ \ldots\ m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.
12. **(a)** If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is a n-cycle σ $(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.
    (b) If $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is an n-cycle σ $(n \geq 5)$ with $\tau = \sigma^k$ for some integer k.
13. Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.
14. Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.
15. Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition. [Use Exercise 10 and Exercise 24 of Section 1.]
16. Show that if $n \geq m$ then the number of m-cycles in S_n is given by
$$\frac{n(n-1)(n-2)\ldots(n-m+1)}{m}.$$
[Count the number of ways of forming an m-cycle and divide by the number of representations of a particular m-cycle.]

17. Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.
18. Find all numbers n such that S_5 contains an element of order n. [Use Exercise 15.]
19. Find all numbers n such that S_7 contains an element of order n. [Use Exercise 15.]
20. Find a set of generators and relations for S_3.

Multiplication is easy when one uses the cycle notation. For example, let us compute $\gamma = \alpha\beta$, where $\alpha = (1\ 2)$ and $\beta = (1\ 3\ 4\ 2\ 5)$. Since multiplication is composition of functions, $\gamma(1) = \alpha \circ \beta(1) = \alpha(\beta(1)) = \alpha(3) = 3$; Next, $\gamma(3) = \alpha(\beta(3)) = \alpha(4) = 4$, and $\gamma(4) = \alpha(\beta(4)) = \alpha(2) = 1$. Having returned to 1, we now seek $\gamma(2)$, because 2 is the smallest integer for which γ has not yet been evaluated. We end up with

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

The cycles on the right are *disjoint* as defined below.

Definition. Two permutations $\alpha, \beta \in S_X$ are ***disjoint*** if every x moved by one is fixed by the other. In symbols, if $\alpha(x) \neq x$, then $\beta(x) = x$ and if $\beta(y) \neq y$, then $\alpha(y) = y$ (of course, it is possible that there is $z \in X$ with $\alpha(z) = z = \beta(z)$). A family of permutations $\alpha_1, \alpha_2, \ldots, \alpha_m$ is ***disjoint*** if each pair of them is disjoint.

Exercises

1.4. Prove that $(1\ 2\ \cdots\ r-1\ r) = (2\ 3\ \cdots\ r\ 1) = (3\ 4\ \cdots\ 1\ 2) = \cdots = (r\ 1 \cdots r-1)$. Conclude that there are exactly r such notations for this r-cycle.

1.5. If $1 \leq r \leq n$, then there are $(1/r)[n(n-1)\ldots(n-r+1)]$ r-cycles in S_n.

1.6. Prove the ***cancellation law*** for permutations: if either $\alpha\beta = \alpha\gamma$ or $\beta\alpha = \gamma\alpha$, then $\beta = \gamma$.

1.7. Let $\alpha = (i_1\ i_2\ \cdots\ i_r)$ and $\beta = (j_1\ j_2\ \cdots\ j_s)$. Prove that α and β are disjoint if and only if $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \varnothing$.

1.8. If α and β are disjoint permutations, then $\alpha\beta = \beta\alpha$; that is, α and β ***commute***.

1.9. If $\alpha, \beta \in S_n$ are disjoint and $\alpha\beta = 1$, then $\alpha = 1 = \beta$.

1.10. If $\alpha, \beta \in S_n$ are disjoint, prove that $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 0$. Is this true if α and β are not disjoint? (Define $\alpha^0 = 1$, $\alpha^1 = \alpha$, and, if $k \geq 2$, define α^k to be the composite of α with itself k times.)

1.11. Show that a power of a cycle need not be a cycle.

1.12. (i) Let $\alpha = (i_0\ i_1\ \ldots\ i_{r-1})$ be an r-cycle. For every $j, k \geq 0$, prove that $\alpha^k(i_j) = i_{k+j}$ if subscripts are read modulo r.
(ii) Prove that if α is an r-cycle, then $\alpha^r = 1$, but that $\alpha^k \neq 1$ for every positive integer $k < r$.
(iii) If $\alpha = \beta_1\beta_2\ldots\beta_m$ is a product of disjoint r_i-cycles β_i, then the smallest positive integer l with $\alpha^l = 1$ is the least common multiple of $\{r_1, r_2, \ldots, r_m\}$.

1.13. (i) A permutation $\alpha \in S_n$ is ***regular*** if either α has no fixed points and it is the product of disjoint cycles of the same length or $\alpha = 1$. Prove that α is regular if and only if α is a power of an n-cycle β; that is, $\alpha = \beta^m$ for some m. (*Hint*: if $\alpha = (a_1a_2\ldots a_k)(b_1b_2\ldots b_k)\ldots(z_1z_2\ldots z_k)$, where there are m letters $a, b, \ldots, z$, then let $\beta = (a_1b_1\ldots z_1a_2b_2\ldots z_2\ldots a_kb_k\ldots z_k)$.)
(ii) If α is an n-cycle, then α^k is a product of (n, k) disjoint cycles, each of length $n/(n, k)$. (Recall that (n, k) denotes the gcd of n and k.)
(iii) If p is a prime, then every power of a p-cycle is either a p-cycle or 1.

1.14. (i) Let $\alpha = \beta\gamma$ in S_n, where β and γ are disjoint. If β moves i, then $\alpha^k(i) = \beta^k(i)$ for all $k \geq 0$.

(ii) Let α and β be cycles in S_n (we do not assume that they have the same length). If there is i_1 moved by both α and β and if $\alpha^k(i_1) = \beta^k(i_1)$ for all positive integers k, then $\alpha = \beta$.