13. Symmetric groups

13.1 Cycles, disjoint cycle decompositions
13.2 Adjacent transpositions
13.3 Worked examples

1. Cycles, disjoint cycle decompositions

The symmetric group $S_n$ is the group of bijections of $\{1, \ldots, n\}$ to itself, also called permutations of $n$ things. A standard notation for the permutation that sends $i \rightarrow \ell_i$ is

$$\left( \begin{array}{cccc} 1 & 2 & 3 & \ldots & n \\ \ell_1 & \ell_2 & \ell_3 & \ldots & \ell_n \end{array} \right)$$

Under composition of mappings, the permutations of $\{1, \ldots, n\}$ is a group.

The fixed points of a permutation $f$ are the elements $i \in \{1, 2, \ldots, n\}$ such that $f(i) = i$.

A $k$-cycle is a permutation of the form

$$f(\ell_1) = \ell_2 \quad f(\ell_2) = \ell_3 \quad \ldots \quad f(\ell_{k-1}) = \ell_k \quad \text{and} \quad f(\ell_k) = \ell_1$$

for distinct $\ell_1, \ldots, \ell_k$ among $\{1, \ldots, n\}$, and $f(i) = i$ for $i$ not among the $\ell_j$. There is standard notation for this cycle:

$$(\ell_1 \ell_2 \ell_3 \ldots \ell_k)$$

Note that the same cycle can be written several ways, by cyclically permuting the $\ell_j$: for example, it also can be written as

$$(\ell_2 \ell_3 \ldots \ell_k \ell_1) \quad \text{or} \quad (\ell_3 \ell_4 \ldots \ell_k \ell_1 \ell_2)$$

Two cycles are disjoint when the respective sets of indices properly moved are disjoint. That is, cycles $(\ell_1 \ell_2 \ell_3 \ldots \ell_k)$ and $(\ell'_1 \ell'_2 \ell'_3 \ldots \ell'_k)$ are disjoint when the sets $\{\ell_1, \ell_2, \ldots, \ell_k\}$ and $\{\ell'_1, \ell'_2, \ldots, \ell'_k\}$ are disjoint.

[1.0.1] Theorem: Every permutation is uniquely expressible as a product of disjoint cycles.

191
Proof: Given $g \in S_n$, the cyclic subgroup $\langle g \rangle \subset S_n$ generated by $g$ acts on the set $X = \{1, \ldots, n\}$ and decomposes $X$ into disjoint orbits

$$O_x = \{g^i x : i \in \mathbb{Z}\}$$

for choices of orbit representatives $x \in X$. For each orbit representative $x$, let $N_x$ be the order of $g$ when restricted to the orbit $\langle g \rangle \cdot x$, and define a cycle

$$C_x = (x g x g^2 x \ldots g^{N_x-1}x)$$

Since distinct orbits are disjoint, these cycles are disjoint. And, given $y \in X$, choose an orbit representative $x$ such that $y \in \langle g \rangle \cdot x$. Then $g \cdot y = C_x \cdot y$. This proves that $g$ is the product of the cycles $C_x$ over orbit representatives $x$.

2. Transpositions

The (adjacent) transpositions in the symmetric group $S_n$ are the permutations $s_i$ defined by

$$s_i(j) = \begin{cases} 
  i+1 & \text{(for } j = i \text{)} \\
  i & \text{(for } j = i+1 \text{)} \\
  j & \text{(otherwise)}
\end{cases}$$

That is, $s_i$ is a 2-cycle that interchanges $i$ and $i+1$ and does nothing else.

[2.0.1] Theorem: The permutation group $S_n$ on $n$ things $\{1,2,\ldots,n\}$ is generated by adjacent transpositions $s_i$.

Proof: Induction on $n$. Given a permutation $p$ of $n$ things, we show that there is a product $q$ of adjacent transpositions such that $(q \circ p)(n) = n$. Then $q \circ p$ can be viewed as a permutation in $S_{n-1}$, and we do induction on $n$. We may suppose $p(n) = i < n$, or else we already have $p(n) = n$ and we can do the induction on $n$.

Do induction on $i$ to get to the situation that $(q \circ p)(n) = n$ for some product $q$ of adjacent transposition. Suppose we have a product $q$ of adjacent transpositions such that $(q \circ p)(n) = i < n$. For example, the empty product $q$ gives $q \circ p = p$. Then $(s_i \circ q \circ p)(n) = i+1$. By induction on $i$ we’re done.

The length of an element $g \in S_n$ with respect to the generators $s_1, \ldots, s_{n-1}$ is the smallest integer $\ell$ such that

$$g = s_{i_1} s_{i_2} \cdots s_{i_{\ell-1}} s_{i_\ell}$$
3. Worked examples

[13.1] Classify the conjugacy classes in $S_n$ (the symmetric group of bijections of $\{1, \ldots, n\}$ to itself).

Given $g \in S_n$, the cyclic subgroup $\langle g \rangle$ generated by $g$ certainly acts on $X = \{1, \ldots, n\}$ and therefore decomposes $X$ into orbits

$$O_x = \{g^i x : i \in \mathbb{Z}\}$$

for choices of orbit representatives $x_i \in X$. We claim that the (unordered!) list of sizes of the (disjoint!) orbits of $g$ on $X$ uniquely determines the conjugacy class of $g$, and vice versa. (An unordered list that allows the same thing to appear more than once is a multiset. It is not simply a set!)

To verify this, first suppose that $g = t h t^{-1}$. Then $\langle g \rangle$-orbits and $\langle h \rangle$-orbits are related by

$$\langle g \rangle\text{-orbit } O_x \leftrightarrow \langle h \rangle\text{-orbit } O_x$$

Indeed,

$$g^\ell \cdot (tx) = (th^{-1})^\ell \cdot (tx) = t(h^\ell \cdot x)$$

Thus, if $g$ and $h$ are conjugate, the unordered lists of sizes of their orbits must be the same.

On the other hand, suppose that the unordered lists of sizes of the orbits of $g$ and $h$ are the same. Choose an ordering of orbits of the two such that the cardinalities match up:

$$|O_x^{(g)}| = |O_y^{(h)}| \quad (\text{for } i = 1, \ldots, m)$$

where $O_x^{(g)}$ is the $\langle g \rangle$-orbit containing $x_i$ and $O_y^{(h)}$ is the $\langle g \rangle$-orbit containing $y_i$. Fix representatives as indicated for the orbits. Let $p$ be a permutation such that, for each index $i$, $p$ bijects $O_x^{(g)}$ to $O_y^{(h)}$ by

$$p(g^i x_i) = h^i y_i$$

The only slightly serious point is that this map is well-defined, since there are many exponents $\ell$ which may give the same element. And, indeed, it is at this point that we use the fact that the two orbits have the same cardinality: we have

$$O_x^{(g)} \leftrightarrow \langle g \rangle / O_x \quad (\text{by } g^\ell (g) x_i \leftrightarrow g^\ell x_i)$$

where $\langle g \rangle x_i$ is the isotropy subgroup of $x_i$. Since $\langle g \rangle$ is cyclic, $\langle g \rangle x_i$ is necessarily $\langle g^N \rangle$ where $N$ is the number of elements in the orbit. The same is true for $h$, with the same $N$. That is, $g^\ell x_i$ depends exactly on $\ell \mod N$, and $h^i y_i$ likewise depends exactly on $\ell \mod N$. Thus, the map $p$ is well-defined.

Then claim that $g$ and $h$ are conjugate. Indeed, given $x \in X$, take $O_x^{(g)}$ containing $x = g^i x_i$ and $O_y^{(h)}$ containing $p x = h^i y_i$. The fact that the exponents of $g$ and $h$ are the same is due to the definition of $p$. Then

$$p(gx) = p(g \cdot g^\ell x_i) = h^{i+\ell} y_i = h \cdot h^\ell y_i = h \cdot p(g^\ell x_i) = h(px)$$

Thus, for all $x \in X$

$$(p \circ g)(x) = (h \circ p)(x)$$

Therefore,

$$p \circ g = h \circ p$$

or

$$pgp^{-1} = h$$

(Yes, there are usually many different choices of $p$ which accomplish this. And we could also have tried to say all this using the more explicit cycle notation, but it’s not clear that this would have been a wise choice.)
[13.2] The projective linear group \( PGL_n(k) \) is the group \( GL_n(k) \) modulo its center \( k \), which is the collection of scalar matrices. Prove that \( PGL_2(\mathbb{F}_3) \) is isomorphic to \( S_4 \), the group of permutations of 4 things. (Hint: Let \( PGL_2(\mathbb{F}_3) \) act on lines in \( \mathbb{F}_3^2 \), that is, on one-dimensional \( \mathbb{F}_3 \)-subspaces in \( \mathbb{F}_3^2 \).)

The group \( PGL_2(\mathbb{F}_3) \) acts by permutations on the set \( X \) of lines in \( \mathbb{F}_3^2 \), because \( GL_2(\mathbb{F}_3) \) acts on non-zero vectors in \( \mathbb{F}_3^2 \). The scalar matrices in \( GL_2(\mathbb{F}_3) \) certainly stabilize every line (since they act by scalars), so act trivially on the set \( X \).

On the other hand, any non-scalar matrix \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) acts non-trivially on some line. Indeed, if

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} * \\ 0 \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix}
\]

then \( c = 0 \). Similarly, if

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ * \end{pmatrix} = \begin{pmatrix} 0 \\ * \end{pmatrix}
\]

then \( b = 0 \). And if

\[
\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\]

for some \( \lambda \) then \( a = d \), so the matrix is scalar.

Thus, the map from \( GL_2(\mathbb{F}_3) \) to permutations \( \text{Aut}_\text{set}(X) \) of \( X \) has kernel consisting exactly of scalar matrices, so factors through (that is, is well defined on) the quotient \( PGL_2(\mathbb{F}_3) \), and is injective on that quotient. (Since \( PGL_2(\mathbb{F}_3) \) is the quotient of \( GL_2(\mathbb{F}_3) \) by the kernel of the homomorphism to \( \text{Aut}_\text{set}(X) \), the kernel of the mapping induced on \( PGL_2(\mathbb{F}_3) \) is trivial.)

Computing the order of \( PGL_2(\mathbb{F}_3) \) gives

\[
|PGL_2(\mathbb{F}_3)| = |GL_2(\mathbb{F}_3)|/|\text{scalar matrices}| = \frac{(3^2 - 1)(3^2 - 3)}{3 - 1} = (3 + 1)(3^2 - 3) = 24
\]

(The order of \( GL_n(\mathbb{F}_q) \) is computed, as usual, by viewing this group as automorphisms of \( \mathbb{F}^n_q \).)

This number is the same as the order of \( S_4 \), and, thus, an injective homomorphism must be surjective, hence, an isomorphism.

(One might want to verify that the center of \( GL_n(\mathbb{F}_q) \) is exactly the scalar matrices, but that’s not strictly necessary for this question.)

[13.3] An automorphism of a group \( G \) is inner if it is of the form \( g \mapsto xgx^{-1} \) for fixed \( x \in G \). Otherwise it is an outer automorphism. Show that every automorphism of the permutation group \( S_3 \) on 3 things is inner. (Hint: Compare the action of \( S_3 \) on the set of 2-cycles by conjugation.)

Let \( G \) be the group of automorphisms, and \( X \) the set of 2-cycles. We note that an automorphism must send order-2 elements to order-2 elements, and that the 2-cycles are exactly the order-2 elements in \( S_3 \). Further, since the 2-cycles generate \( S_3 \), if an automorphism is trivial on all 2-cycles it is the trivial automorphism. Thus, \( G \) injects to \( \text{Aut}_\text{set}(X) \), which is permutations of 3 things (since there are three 2-cycles).

On the other hand, the conjugation action of \( S_3 \) on itself stabilizes \( X \), and, thus, gives a group homomorphism \( f : S_3 \to \text{Aut}_\text{set}(X) \). The kernel of this homomorphism is trivial: if a non-trivial permutation \( p \) conjugates the two-cycle \( t = (1 \ 2) \) to itself, then

\[
(ptp^{-1})(3) = t(3) = 3
\]

so \( tp^{-1}(3) = p^{-1}(3) \). That is, \( t \) fixes the image \( p^{-1}(3) \), which therefore is 3. A symmetrical argument shows that \( p^{-1}(i) = i \) for all \( i \), so \( p \) is trivial. Thus, \( S_3 \) injects to permutations of \( X \).
In summary, we have group homomorphisms

\[ S_3 \longrightarrow \text{Aut}_{\text{group}}(S_3) \longrightarrow \text{Aut}_{\text{set}}(X) \]

where the map of automorphisms of $S_3$ to permutations of $X$ is an isomorphism, and the composite map of $S_3$ to permutations of $X$ is surjective. Thus, the map of $S_3$ to its own automorphism group is necessarily surjective.

[13.4] Identify the element of $S_n$ requiring the maximal number of adjacent transpositions to express it, and prove that it is unique.

We claim that the permutation that takes $i \mapsto n - i + 1$ is the unique element requiring $n(n - 1)/2$ elements, and that this is the maximum number.

For an ordered listing $(t_1, \ldots, t_n)$ of $\{1, \ldots, n\}$, let

\[ d_o(t_1, \ldots, t_n) = \text{number of indices } i < j \text{ such that } t_i > t_j \]

and for a permutation $p$ let

\[ d(p) = d_o(p(1), \ldots, p(n)) \]

Note that if $t_i < t_j$ for all $i < j$, then the ordering is $(1, \ldots, n)$. Also, given a configuration $(t_1, \ldots, t_n)$ with some $t_i > t_j$ for $i < j$, necessarily this inequality holds for some adjacent indices (or else the opposite inequality would hold for all indices, by transitivity). Thus, if the ordering is not the default $(1, \ldots, n)$, then there is an index $i$ such that $t_i > t_{i+1}$. Then application of the adjacent transposition $s_i$ of $i, i + 1$ reduces by exactly 1 the value of the function $d_o()$.

Thus, for a permutation $p$ with $d(p) = \ell$ we can find a product $q$ of exactly $\ell$ adjacent transpositions such that $q \circ p = 1$. That is, we need at most $d(p) = \ell$ adjacent transpositions to express $p$. (This does not preclude less efficient expressions.)

On the other hand, we want to be sure that $d(p) = \ell$ is the minimum number of adjacent transpositions needed to express $p$. Indeed, application of $s_i$ only affects the comparison of $p(i)$ and $p(i + 1)$. Thus, it can decrease $d(p)$ by at most 1. That is,

\[ d(s_i \circ p) \geq d(p) - 1 \]

and possibly $d(s_i \circ p) = d(p)$. This shows that we do need at least $d(p)$ adjacent transpositions to express $p$.

Then the permutation $w_o$ that sends $i$ to $n - i + 1$ has the effect that $w_o(i) > w_o(j)$ for all $i < j$, so it has the maximum possible $d(w_o) = n(n - 1)/2$. For uniqueness, suppose $p(i) > p(j)$ for all $i < j$. Evidently, we must claim that $p = w_o$. And, indeed, the inequalities

\[ p(n) < p(n - 1) < p(n - 2) < \ldots < p(2) < p(1) \]

leave no alternative (assigning distinct values in $\{1, \ldots, n\}$) but

\[ p(n) = 1 < p(n - 1) = 2 < \ldots < p(2) = n - 1 < p(1) = n \]

(One might want to exercise one’s technique by giving a more careful inductive proof of this.)

[13.5] Let the permutation group $S_n$ on $n$ things act on the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ by $\mathbb{Z}$-algebra homomorphisms defined by $p(x_i) = x_{p(i)}$ for $p \in S_n$. (The universal mapping property of the polynomial ring allows us to define the images of the indeterminates $x_i$ to be whatever we want, and at the same time guarantees that this determines the $\mathbb{Z}$-algebra homomorphism completely.) Verify that this is a group homomorphism

\[ S_n \longrightarrow \text{Aut}_{\mathbb{Z}-\text{alg}}(\mathbb{Z}[x_1, \ldots, x_n]) \]
Consider
\[ D = \prod_{i<j} (x_i - x_j) \]
Show that for any \( p \in S_n \)
\[ p(D) = \sigma(p) \cdot D \]
where \( \sigma(p) = \pm 1 \). Infer that \( \sigma \) is a (non-trivial) group homomorphism, the sign homomorphism on \( S_n \).

Since these polynomial algebras are free on the indeterminates, we check that the permutation group acts (in the technical sense) on the set of indeterminates. That is, we show associativity and that the identity of the group acts trivially. The latter is clear. For the former, let \( p, q \) be two permutations. Then
\[ (pq)(x_i) = x_{(pq)(i)} \]
while
\[ p(q(x_i)) = p(x_{q(i)} = x_{p(q(i))} \]
Since \( p(q(i)) = (pq)(i) \), each \( p \in S_n \) gives an automorphism of the ring of polynomials. (The endomorphisms are invertible since the group has inverses, for example.)

Any permutation merely permutes the factors of \( D \), up to sign. Since the group acts in the technical sense,
\[ (pq)(D) = p(q(D)) \]
That is, since the automorphisms given by elements of \( S_n \) are \( \mathbb{Z} \)-linear,
\[ \sigma(pq) \cdot D = p(\sigma(q) \cdot D) = \sigma(q)p(D) = \sigma(q) \cdot \sigma(p) \cdot D \]
Thus,
\[ \sigma(pq) = \sigma(p) \cdot \sigma(q) \]
which is the homomorphism property of \( \sigma \).

Exercises

13.[3.0.1] How many distinct \( k \)-cycles are there in the symmetric group \( S_n \)?
13.[3.0.2] How many elements of order 35 are there in the symmetric group \( S_{12} \)?
13.[3.0.3] What is the largest order of an element of \( S_{12} \)?
13.[3.0.4] How many elements of order 6 are there in the symmetric group \( S_{11} \)?
13.[3.0.5] Show that the order of a permutation is the least common multiple of the lengths of the cycles in a disjoint cycle decomposition of it.
13.[3.0.6] Let \( X \) be the set \( \mathbb{Z}/31 \), and let \( f : X \to X \) be the permutation \( f(x) = 2 \cdot x \). Decompose this permutation into disjoint cycles.
13.[3.0.7] Let \( X \) be the set \( \mathbb{Z}/29 \), and let \( f : X \to X \) be the permutation \( f(x) = x^3 \). Decompose this permutation into disjoint cycles.
13.[3.0.8] Show that if a permutation is expressible as a product of an odd number of 2-cycles in one way, then any expression of it as a product of 2-cycles expresses it as a product of an odd number of 2-cycles.
13.[3.0.9] Identify the lengths (expressed in terms of adjacent transpositions) of all the elements in \( S_4 \).
13.[3.0.10] (*) Count the number of elements of \( S_n \) having at least one fixed point.