Chapter 3. The Symmetric and Alternating Groups

3.1 Definition: An element $\alpha \in S_n$ can be specified by giving its table of values in the form

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

This is called **array notation** for α.

3.2 Example: In array notation, we have

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Note that S_3 is not abelian because for example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \ , \ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

(since the operation is composition, in the product $\alpha\beta$, the permutation β is performed before the permutation α).

3.3 Example: For $n \geq 3$, we can think of D_n as a subgroup of S_n because an element of D_n permutes the elements of $C_n = \left\{ e^{i\,2\pi k/n} \middle| k = 1, 2, \cdots, n \right\}$ and this determines a permutation of $\{1, 2, \cdots, n\}$. For example, in D_6 we have

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \ , \ R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

$$F_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} \ , \ F_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

3.4 Definition: When $a_1, a_2, \cdots, a_\ell$ are distinct elements in $\{1, 2, \cdots, n\}$ we write

$$\alpha = (a_1, a_2, \cdots, a_\ell)$$

for the permutation $\alpha \in S_n$ given by

$$\begin{aligned} &\alpha(a_1) = a_2 \ , \ \alpha(a_2) = a_3 \ , \ \cdots \ , \ \alpha(a_{\ell-1}) = a_\ell \ , \ \alpha(a_\ell) = a_1 \\ &\alpha(k) = k \text{ for all } k \notin \{a_1, a_2, \cdots, a_\ell\}. \end{aligned}$$

Such a permutation is called a **cycle of length** ℓ or an ℓ**-cycle**.

3.5 Note: We make several remarks.

(1) We have $e = (1) = (2) = \cdots = (n)$.
(2) We have $(a_1, a_2, \cdots, a_\ell) = (a_2, a_3, \cdots, a_\ell, a_1) = (a_3, a_4, \cdots, a_\ell, a_1, a_2) = \cdots$.
(3) An ℓ-cycle with $\ell \geq 2$ can be expressed *uniquely* in the form $\alpha = (a_1, a_2, \cdots, a_\ell)$ with $a_1 = \min\{a_1, a_2, \cdots, a_\ell\}$.
(4) For an ℓ-cycle $\alpha = (a_1, a_2, \cdots, a_\ell)$ we have $|\alpha| = \ell$.
(5) If $n \geq 3$ then we have $(12)(23) = (123)$ and $(23)(12) = (132)$ so S_n is not abelian.

3.6 Definition: Two cycles $\alpha = (a_1, a_2, \cdots, a_\ell)$ and $\beta = (b_1, b_2, \cdots, b_m)$ are said to be **disjoint** when $\{a_1, \cdots, a_\ell\} \cap \{b_1, \cdots, b_m\} = \emptyset$, that is when the a_i and b_j are all distinct. More generally the cycles $\alpha_1 = (a_{1,1}, \cdots, a_{1,\ell_1}), \cdots, \alpha_m = (a_{m,1}, \cdots, a_{m,\ell_m})$ are **disjoint** when all of the $a_{i,j}$ are distinct.

3.7 Note: Disjoint cycles commute. Indeed if $\alpha = (a_1, \cdots, a_\ell)$ and $\beta = (b_1, \cdots, b_m)$ are disjoint, then

$$\begin{aligned} \alpha\big(\beta(a_i)\big) &= \alpha(a_i) = a_{i+1} = \beta(a_{i+1}) = \beta\big(\alpha(a_i)\big) \text{ , with subscripts in } \mathbb{Z}_\ell \\ \alpha\big(\beta(b_j)\big) &= \alpha(b_{j+1}) = b_{j+1} = \beta(b_j) = \beta\big(\alpha(b_j)\big) \text{ , with subscripts in } \mathbb{Z}_m \\ \alpha\big(\beta(k)\big) &= \alpha(k) = k = \beta(k) = \beta\big(\alpha(k)\big) \text{ for } k \neq a_i, b_j \,. \end{aligned}$$

3.8 Theorem: (*Cycle Notation*) *Every $\alpha \in S_n$ can be written as a product of disjoint cycles. Indeed every $\alpha \neq e$ can be written uniquely in the form*

$$\alpha = (a_{1,1}, \cdots, a_{1,\ell_1})(a_{2,1}, \cdots, a_{2,\ell_2}) \cdots (a_{m,1}, \cdots, a_{m,\ell_m})$$

with $m \geq 1$, each $\ell_i \geq 2$, each $a_{i,1} = \min\{a_{i,1}, a_{i,2}, \cdots, a_{i,\ell_i}\}$ and $a_{1,1} < a_{2,1} < \cdots < a_{m,1}$.

Proof: Let $e \neq \alpha \in S_n$ where $n \geq 2$. To write α in the given form, we must take $a_{1,1}$ to be the smallest element $k \in \{1, 2, \cdots, n\}$ with $\alpha(k) \neq k$. Then we must have $a_{1,2} = \alpha(a_{1,1})$, $a_{1,3} = \alpha(a_{1,2}) = \alpha^2(a_{1,1})$, and so on. Eventually we must reach ℓ_1 such that $a_{1,1} = \alpha^{\ell_1}(a_{1,1})$, indeed since $\{1, 2, \cdots, n\}$ is finite, eventually we find $\alpha^i(a_{1,1}) = \alpha^j(a_{1,1})$ for some $1 \leq i < j$ and then $a_{1,1} = \alpha^{-i}\alpha^i(a_{1,1}) = \alpha^{-i}\alpha^j(a_{1,1}) = \alpha^{j-i}(a_{1,1})$. For the smallest such ℓ_1 the elements $a_{1,1}, \cdots, a_{1,\ell_1}$ will be disjoint since if we had $a_{1,i} = a_{1,j}$ for some $1 \leq i < j \leq \ell_1$ then, as above, we would have $\alpha^{j-i}(a_{11}) = a_{11}$ with $1 \leq j - i < \ell_1$. This gives us the first cycle $\alpha_1 = (a_{1,1}, a_{1,2}, \cdots, a_{1,\ell_1})$.

If we have $\alpha = \alpha_1$ we are done. Otherwise there must be some $k \in \{1, 2, \cdots, n\}$ with $k \notin \{a_{1,1}, a_{1,2}, \cdots, a_{1,\ell_1}\}$ such that $\alpha(k) \neq k$, and we must choose $a_{2,1}$ to be the smallest such k. As above we obtain the second cycle $\alpha_2 = (a_{2,1}, a_{2,2}, \cdots, a_{2,\ell_2})$. Note that α_2 must be disjoint from α_1 because if we had $\alpha^i(a_{2,1}) = \alpha^j(a_{1,1})$ for some i, j then we would have $a_{2,1} = \alpha^{-i}\alpha^i(a_{2,1}) = \alpha^{-i}\alpha^j(a_{1,1}) = \alpha^{j-i}(a_{1,1}) \in \{a_{1,1}, \cdots, a_{1,\ell_1}\}$.

At this stage, if $\alpha = \alpha_1\alpha_2$ we are done, and otherwise we continue the procedure.

3.9 Definition: When a permutation $e \neq \alpha \in S_n$ is written in the unique form of the above theorem, we say that α is written in **cycle notation**. We usually write e as $e = (1)$.

3.10 Example: In cycle notation we have

$$\begin{aligned} S_3 = D_3 &= \big\{(1), (12), (13), (23), (123), (132)\big\} \\ S_4 &= \big\{(1), (12), (13), (14), (23), (24), (34),\ (12)(34)\ ,\ (13)(24)\ ,\ (14)(23)\ , \\ &\qquad (123), (132), (124), (142), (134), (143), (234), (243), \\ &\qquad (1234), (1243), (1324), (1342), (1423), (1432)\big\} \\ D_4 &= \big\{I, R_1, R_2, R_3.R_4, R_5, F_0, F_1, F_2, F_3, F_4, F_5\big\} \\ &= \big\{(1), (1234)\ ,\ (13)(24)\ ,\ (1432)\ ,\ (13)\ ,\ (14)(23)\ ,\ (24)\ ,\ (12)(34)\big\} \end{aligned}$$

3.11 Example: For $\alpha = (1352)(46)$, $\beta = (145)(263) \in S_6$, express $\alpha\beta$ in cycle notation.

3.12 Example: Find the number of elements in S_{15} which can be written as a product of 3 disjoint 4-cycles.

Solution: When we write $\alpha = (a_1a_2a_3a_4)(a_5a_6a_7a_8)(a_9a_{10}a_{11}a_{12})$, there are $\binom{15}{12}$ ways to choose the set $\{a_1, \cdots, a_{12}\}$ from $\{1, 2, \cdots, 15\}$, then there is one choice for a_1 (it must be the smallest of the a_i), then there are 11 choices for a_2, then 10 choices for a_3, then 9 choices for a_4, and then there is only one choice for a_5 (it must be the smallest of the remaining a_i, and so on. Thus there are $\binom{15}{12} \cdot \frac{12!}{12\cdot 8\cdot 4}$ such elements in S_{15}.

3.13 Example: Find the number of elements in S_{20} which can be written as a product of 7 disjoint cycles, with 4 of length 2, 2 of length 3, and 1 of length 4.

Solution: When we write $\alpha = (a_1a_2)(a_3a_4)(a_5a_6)(a_7a_8)\,(b_1b_2b_3)(b_4b_5b_6)\,(c_1c_2c_3c_4)$, there are $\binom{20}{8}$ ways to choose $\{a_1, a_2, \cdots, a_8\}$ from $\{1, 2, \cdots, 20\}$, then $\binom{12}{6}$ ways to choose $\{b_1, \cdots, b_6\}$ from $\{1, \cdots, 20\} \setminus \{a_1, \cdots, a_8\}$, and then there are $\binom{4}{4} = 1$ way to choose $\{c_1, \cdots, c_4)\}$. From the set $\{a_1, \cdots, a_8\}$, there is 1 way to choose a_1, then 7 ways to choose a_2, then 1 way to choose a_3, then 5 ways to choose a_4, then 1 way to choose a_5, then 3 ways to choose a_6, then 1 way to choose a_7 and then 1 way to choose a_8. From the set $\{b_1, \cdots, b_6\}$, there is 1 way to choose b_1, then 5 ways to choose b_2, then 4 ways to choose b_3, then 1 way to choose b_4, then 2 ways to choose b_5 and then 1 way to choose b_6. From the set $\{c_1, \cdots, c_4\}$, there is 1 way to choose c_1, then 3 ways to choose c_2, then 2 ways to choose c_3 and then 1 way to choose c_4. Thus the number of such elements in S_{20} is

$$\binom{20}{8}\binom{12}{6}\binom{4}{4} \cdot \frac{8!}{8\cdot 6\cdot 4\cdot 2} \cdot \frac{6!}{6\cdot 3} \cdot \frac{4!}{4}\,.$$

3.14 Theorem: *(The Order of a Permutation) Let $\alpha = \alpha_1\alpha_2\cdots\alpha_m$ where the α_i are disjoint cycles with each α_i of length ℓ_i. Then $|\alpha| = \mathrm{lcm}\{\ell_1, \cdots, \ell_m\}$.*

Proof: Since the α_i are disjoint, if we write $\alpha_k = (a_{k,1}, \cdots, a_{k,\ell_k})$ then we have

$$\alpha(a_{k,1}) = a_{k,2}\ ,\ \alpha^2(a_{k,1}) = a_{k,3}\ ,\ \cdots\ ,\ \alpha^{\ell_m-1}(a_{k,1}) = a_{k,\ell_m}\ ,\ \alpha^{\ell_m}(a_{k,1}) = a_{k,1}\,.$$

If p is a common multiple of all the ℓ_i, say $p = \ell_i q_i$, then

$$\alpha_i{}^p = \alpha_i{}^{\ell_i q_i} = (\alpha_i{}^{\ell_i})^{q_i} = e^{q_i} = e \text{ for all } i\,.$$

Since the α_i commute, we have $\alpha^p = (\alpha_1\alpha_2\cdots\alpha_m)^p = \alpha_1{}^p\alpha_2{}^p\cdots\alpha_m{}^p = e$.

If, on the other hand, p is not a common multiple of the ℓ_i, then we can choose k so that p is not a multiple of ℓ_k. Write $p = \ell_k q + r$ with $0 < r < \ell_k$. Then

$$\alpha_k{}^p = \alpha_k{}^{\ell_k q + r} = (\alpha_k{}^{\ell_k})^{q_k}\alpha_k{}^r = \alpha_k{}^r$$

and we have $\alpha^p(a_{k,1}) = \alpha_k{}^p(a_{k,1}) = \alpha_k{}^r(a_{k,1}) \neq a_{k,1}$ since $0 < r < \ell_k$, and so $\alpha^p \neq e$.

3.15 Theorem: *(The Conjugacy Class of a Permutation) Let $\alpha, \beta \in S_n$. Then α and β are conjugate in S_n if and only if, when written in cycle notation, α and β have the same number of cycles of each length.*

Proof: Write α in cycle notation as $\alpha = (a_{11}, a_{12}, \cdots, a_{1,\ell_1})\cdots(a_{m1}, a_{m2}, \cdots, a_{m,\ell_m})$. Note that for all $\sigma \in S_n$ we have

$$\sigma\alpha\sigma^{-1} = \big(\sigma(a_{11}), \sigma(a_{12}), \cdots, \sigma(a_{1,\ell_1})\big)\cdots\big(\sigma(a_{m1}), \sigma(a_{m2}), \cdots, \sigma(a_{m,\ell_m})\big).$$

Indeed, for the permutation on the right, $\sigma(a_{i,j})$ is sent to $\sigma(a_{i,j+1})$, and on the left, $\sigma(a_{i,j})$ is sent by σ to $a_{i,j}$, which is then sent to $a_{i,j+1}$ by α, which is then sent by σ to $\sigma(a_{i,j+1})$.

3.16 Example: Let $\alpha = (1693)(275)(15873) \in S_{10}$. Find $|\alpha|$.

Solution: First we write α in as a product of *disjoint* cycles. We have $\alpha = (127)(369)(58)$ and so $|\alpha| = \mathrm{lcm}(3, 3, 2) = 6$.

3.17 Example: As an exercise, find the number of elements of each order in S_6.

3.18 Theorem: (*Even and Odd Permutations*) *In S_n, with $n \geq 2$,*
(1) every $\alpha \in S_n$ is a product of 2-cycles,
(2) if $e = (a_1, b_1)(a_2, b_2) \cdots (a_\ell, b_\ell)$ then ℓ is even, that is $\ell = 0$ mod 2, and
(3) if $\alpha = (a_1, b_1)(a_2, b_2) \cdots (a_\ell, b_\ell) = (c_1, d_1)(c_2, d_2) \cdots (c_m, d_m)$ then $\ell = m \mod 2$.

Solution: To prove part (1), note that given $\alpha \in S_n$ we can write α as a product of cycles, and we have

$$(a_1, a_2, \cdots, a_\ell) = (a_1, a_\ell)(a_1, a_{\ell-1}) \cdots (a_1, a_2) .$$

We shall prove part (2) by induction. First note that we cannot write e as a single 2-cycle, but we can write e as a product of two 2-cycles, for example $e = (1, 2)(1, 2)$. Fix $\ell \geq 3$ and suppose, inductively, that for all $k < \ell$, if we can write e as a product of k 2-cycles the k must be even. Suppose that e can be written as a product of ℓ 2-cycles, say $e = (a_1, b_1)(a_2, b_2) \cdots (a_\ell, b_\ell)$. Let $a = a_1$. Of all the ways we can write e as a product of ℓ 2-cycles, in the form $e = (x_1, y_1)(x_2, y_2) \cdots (x_\ell, y_\ell)$, with $x_i = a$ for some i, choose one way, say $e = (r_1, s_1)(r_2, s_2) \cdots (r_\ell, s_\ell)$ with $r_m = a$ and $r_i, s_i \neq a$ for all $i < m$, with m being as large as possible. Note that $m \neq \ell$ since for $\alpha = (r_1, s_1) \cdots (r_\ell, s_\ell)$ with $r_\ell = a$ and $r_i, s_i \neq a$ for $i < \ell$ we have $\alpha(s_\ell) = a \neq s_\ell$ and so $\alpha \neq e$. Consider the product $(r_m, s_m)(r_{m+1}, s_{m+1})$. This product must be (after possibly interchanging r_{m+1} and s_{m+1}) of one of the forms

$$(a, b)(a, b) \ , \ (a, b)(a, c) \ , \ (a, b)(b, c) \ , \ (a, b)(c, d)$$

where a, b, c, d are distinct. Note that

$$\begin{aligned} (a, b)(a, c) &= (a, c, b) = (b, c)(a, b), \\ (a, b)(b, c) &= (a, b, c) = (b, c)(a, c), \text{ and} \\ (a, b)(c, d) &= (c, d)(a, b) , \end{aligned}$$

and so in each of these three cases we could rewrite e as a product of ℓ 2-cycles with the first occurrence of a being farther to the right, contradicting the fact that we chose m to be as large as possible. Thus the product $(r_m, s_m)(r_{m+1}, s_{m+1})$ is of the form $(a, b)(a, b)$. By cancelling these two terms, we can write e as a product of $(\ell - 2)$ 2-cycles. By the induction hypothesis, $(\ell - 2)$ is even, and so ℓ is even.

Finally, to prove part (3), suppose that $\alpha = (a_1, b_1) \cdots (a_\ell, b_\ell) = (c_1, d_1) \cdots (c_m, d_m)$. Then we have

$$e = \alpha \, \alpha^{-1} = (a_1, b_1) \cdots (a_\ell, b_\ell)(c_m, d_m) \cdots (c_1, d_1).$$

By part (2), $\ell + m$ is even, and so $\ell = m \mod 2$.

3.19 Example: Show that

$$S_n = \langle (12), (13), (14), \cdots, (1n) \rangle = \langle (12), (23), (34), \cdots, (n-1, n) \rangle = \langle (12), (123 \cdots n) \rangle .$$

Solution: By Part (1) of the above theorem, S_n is generated by the set of all 2-cycles (kl). Any 2-cycle (kl) can be written as $(kl) = (1k)(1l)(1k)$ so $S_n = \langle (12), (13), (14), \cdots, (1n) \rangle$. Any 2-cycle of the form $(1k)$ can be written as $(1k) = (12)(23) \cdots (k-1, k) \cdots (23)(12)$ and so $S_n = \langle (12), (23), \cdots, (n-1, n) \rangle$. Any 2-cycle of the form $(k, k+1)$ can be written as $(k, k+1) = (123 \cdots n)^{k-1}(12)(123 \cdots n)^{-(k-1)}$ and so $S_n = \langle (12)(123 \cdots n) \rangle$.

3.20 Definition: For $n \geq 2$, a permutation $\alpha \in S_n$ is called **even** if it can be written as a product of an even number of 2-cycles. Otherwise α can be written as a product of an odd number of 2-cycles, and then it is called **odd**. We define the **parity** of $\alpha \in S_n$ to be

$$(-1)^\alpha = \begin{cases} \ \ 1 \text{ if } \alpha \text{ is even,} \\ -1 \text{ if } \alpha \text{ is odd.} \end{cases}$$

3.21 Theorem: (*Properties of Parity*) *Let $n \geq 2$ and let $\alpha, \beta \in S_n$. Then*
(1) $(-1)^e = 1$,
(2) if α is an ℓ-cycle then $(-1)^\alpha = (-1)^{\ell-1}$,
(3) $(-1)^{\alpha\beta} = (-1)^\alpha(-1)^\beta$, *and*
(4) $(-1)^{\alpha^{-1}} = (-1)^\alpha$.

Proof: Part (1) holds because, for example, $e = (1,2)(1,2)$. Part (2) holds because we have $(a_1, a_2, \cdots, a_\ell) = (a_1, a_\ell)(a_1, a_{\ell-1}) \cdots (a_1, a_2)$. Part (3) holds because if α is a product of ℓ 2-cycles and β is a product of m 2-cycles then $\alpha\beta$ is a product of $(\ell + m)$ 2-cycles. Part (4) holds because if $\alpha = (a_1, b_1)(a_2, b_2) \cdots (a_\ell, b_\ell)$ then $\alpha^{-1} = (a_\ell, b_\ell) \cdots (a_2, b_2)(a_1, b_1)$.

3.22 Example: Let $\alpha = (1793)(245)(164385) \in S_{10}$. Find $(-1)^\alpha$ and $|\alpha|$.

Solution: By the above theorem, we have $(-1)^\alpha = (-1)^3(-1)^2(-1)^5 = 1$. To find $|\alpha|$, we first write α as a product of *disjoint* cycles. We find that $\alpha = (165793824)$ and so $|\alpha| = 9$.

3.23 Definition: For $n \geq 2$ we define the **alternating group** A_n to be

$$A_n = \left\{\alpha \in S_n \middle| (-1)^\alpha = 1\right\}.$$

Note that $A_n \leq S_n$ by the Properties of Parity Theorem. Note that

$$|A_n| = \tfrac{1}{2}|S_n| = \tfrac{n!}{2}$$

because we have a bijective correspondence

$$F : \left\{\alpha \in S_n \middle| (-1)^\alpha = 1\right\} \to \left\{\alpha \in S_n \middle| (-1)^\alpha = -1\right\}$$

given by $F(\alpha) = (12)\alpha$.

3.24 Remark: The rotation group of the regular tetrahedron can be identified with A_4 by labelling the vertices of the tetrahedron by 1, 2, 3 and 4 and identifying each rotation with a permutation of $\{1, 2, 3, 4\}$.

3.25 Example: Show that A_n is generated by the set of all 3-cycles, then show that for any $a \neq b \in \{1, 2, \cdots, n\}$, A_n is generated by the 3-cycles of the form (abk) with $k \neq a, b$.

Solution: We already know that every permutation in A_n is equal to a product of an even number of 2-cycles. Every product of a pair of 2-cycles is of one of the forms $(ab)(ab)$, $(ab)(ac)$ or $(ab)(cd)$, where a, b, c, d are distinct, and we have

$$(ab)(ab) = (abc)(acb) \ , \ (ab)(ac) = (acb) \ , \ (ab)(cd) = (adc)(abc) \, ,$$

and so A_n is generated by the set of all 3-cycles. Now fix $a, b \in \{1, 2, \cdots, n\}$ with $a \neq b$. Note that every 3-cycle is of one of the forms (abk), (akb), (akl), (bkl) or (klm), where a, b, k, l, m are all distinct, and we have

$$(akb) = (abk)^2 \ , \ (akl) = (abl)(abk)^2 \ , \ (bkl) = (abl)^2(abk) \ , \ (klm) = (abk)^2(abm)(abl)^2(abk) \, .$$