

5 Permutations and Orbits

In the earliest conceptions of group theory, all groups were considered *permutation groups*. Essentially a group was a collection of ways in which one could rearrange some set or object: for example, each ‘rearrangement’ of an equilateral triangle corresponds to one of its *symmetries*. It was Arthur Cayley, of Cayley-table fame, who formulated the group axioms we now use. Importantly, he also proved what is now known as *Cayley’s Theorem*: that the old definition and the new are identical.

5.1 The Symmetric Group

So what, first, is a permutation?

Definition 5.1. A *permutation* of a set A is a bijection $\varphi : A \rightarrow A$.

Theorem 5.2. If A is any set, then the set of permutations S_A of A forms a group under composition.

Proof. We check the axioms:

Closure If φ, ψ are bijective then so is the composition $\varphi \circ \psi$. ✓

Associativity Permutations are functions, the composition of which we know to be associative. ✓

Identity The *identity function* id_A maps all elements of A to themselves: $\text{id}_A : x \mapsto x$. This is certainly bijective. ✓

Inverse If φ is a permutation then it is a bijection, whence the *function* φ^{-1} exists and is also a bijection. ✓ ■

Definition 5.3. The *symmetric group on n -letters* S_n is the group of permutations of any¹ set A of n elements. Typically we choose $A = \{1, 2, \dots, n\}$.

Basic combinatorics should make the following obvious:

Lemma 5.4. S_n has $n!$ elements.²

To describe a group as a *permutation group* simply means that each element of the group is being viewed as a permutation of some set. As the following result shows, all groups are permutation groups, although sadly not in a particularly useful way!

Theorem 5.5 (Cayley’s Theorem). Every group G is isomorphic to a group of permutations.

Proof. For each element $a \in G$, let $\rho_a : G \rightarrow G$ be the function $\rho_a : g \mapsto ag$ (i.e. left multiplication by a). We make two claims:

1. Each ρ_a is a permutation of G .
2. $(\{\rho_a : a \in G\}, \circ)$ forms a group isomorphic to G .

¹ S_n is the *explicit* group of permutations of $\{1, 2, \dots, n\}$ or the *abstract* group of permutations of any set with n elements.

²In contrast to C_n or \mathbb{Z}_n where the subscript is the order of the group.

The first claim is straightforward. $\rho_{a^{-1}}$ is the inverse function to ρ_a :

$$\forall g \in G, (\rho_{a^{-1}} \circ \rho_a)(g) = a^{-1}ag = g = \text{id}_G(g)$$

whence each ρ_a is a bijection.

Now define a map $\phi : G \rightarrow \{\rho_a\}$ by $\phi(a) = \rho_a$. We claim this is an isomorphism:

$$1-1 \quad \phi(a) = \phi(b) \implies \rho_a = \rho_b \implies \forall g \in G, ag = bg \implies a = b. \checkmark$$

Onto Certainly every permutation ρ_a is in the image of ϕ . \checkmark

Homomorphism If $a, b \in G$, then

$$\phi(a) \circ \phi(b) : g \mapsto \rho_a(\rho_b(g)) = abg = \rho_{ab}(g)$$

from which $\phi(ab) = \phi(a) \circ \phi(b)$. \blacksquare

Note that Cayley's Theorem is *not* saying that every group is isomorphic to some S_n . It is saying that every group G is isomorphic to some *subgroup* of S_G .

Three notations for permutations

Standard notation Suppose that $\sigma \in S_4$ is the following map

$$\sigma : \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \mapsto \begin{pmatrix} 3 \\ 1 \\ 4 \\ 2 \end{pmatrix}, \quad \text{i.e. } \sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2$$

We could then write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

where you read down columns to find where σ maps an element in the top row. Composition is read in the usual way for functions, do the right permutation first. Thus if

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \text{then} \quad \sigma\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \quad (*)$$

Matrix Notation σ can also be viewed as acting on the vector $(1, 2, 3, 4)^T$, which suggests a matrix method for encoding elements of S_n . For example, our permutation σ may be written

$$\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

as a *permutation matrix*: multiplying on the left by such a matrix permutes the entries of vectors.

Definition 5.6. A *permutation matrix* is an $n \times n$ matrix with exactly one entry of 1 in each row and column and the remaining entries 0.

Indeed we may conclude:

Theorem 5.7. The set of $n \times n$ permutation matrices forms a group under multiplication which is isomorphic to S_n . By Cayley's Theorem, every finite group of permutations is isomorphic to a group of matrices.

Cycle notation Our example permutation can be more compactly written as $\sigma = (1\ 3\ 4\ 2)$. We read from left to right, looping back to 1 at the end, each entry telling us where the previous is mapped to. Thus $(1\ 3\ 4\ 2)$ maps

$$1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$$

We have shorter cycles if some of the elements are fixed; for example in our two notations

$$(1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \in S_4$$

Juxtaposition is used for composition:

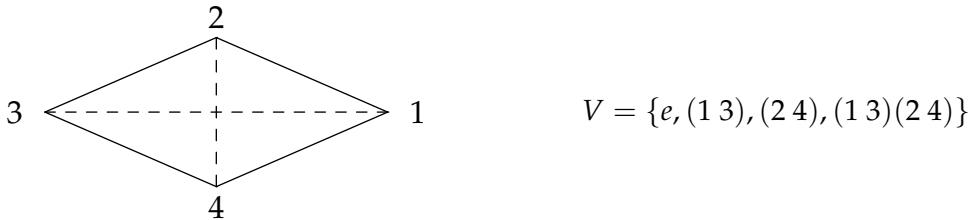
$$(1\ 3\ 4\ 2)(2\ 4) = (1\ 3\ 4)$$

(compare with (*) above).

Remember that multiplication of cycles is really composition of functions: although each *cycle* is read from left to right when determining how it acts on elements of $\{1, 2, \dots, n\}$, we multiply cycles by considering the *rightmost* cycle first. For example, in S_5 ,

$$(1\ 3\ 5\ 4)(2\ 3\ 4) : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 3 \mapsto 5 \\ 3 \mapsto 4 \mapsto 1 \\ 4 \mapsto 2 \\ 5 \mapsto 4 \end{cases} \implies (1\ 3\ 5\ 4)(2\ 3\ 4) = (1\ 3)(2\ 5\ 4) \quad (\dagger)$$

This notation can be used to describe non-symmetric groups: e.g. if we label the corners of a rhombus, the Klein 4-group V can be written in terms of cycles as a subgroup of S_4 .



Definition 5.8. Suppose that $k \leq n$. A k -cycle in S_n is an element $(a_1\ a_2\ \dots\ a_k)$.

Cycles $(a_1\ \dots\ a_k)$ and $(b_1\ \dots\ b_l)$ are *disjoint* if no element appears in both cycles: that is, if

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset$$

The identity element is the only 0-cycle. It is sometimes written $()$, if not otherwise denoted by e .

As the example (\dagger) illustrates, when computing the product of several cycles, the result will typically be a product of disjoint cycles. This will prove very useful in the next section when we discuss *orbits*.

Subgroup relations between symmetric groups It is easy to see that $S_m \leq S_n \iff m \leq n$. For example, fix the final $n - m$ elements of $\{1, \dots, n\}$ so that

$$S_m = \{\sigma \in S_n : \sigma(i) = i, \forall i > m\}.$$

In fact S_m is a subgroup of S_n in precisely $\binom{n}{m}$ different ways: each copy of S_m arises by fixing $n - m$ elements of the set $\{1, \dots, n\}$: there are precisely $\binom{n}{n-m} = \binom{n}{m}$ ways of choosing these fixed elements.

5.2 Dihedral groups

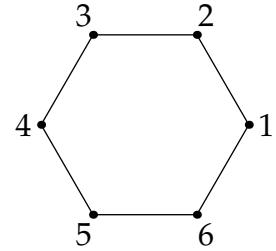
Definition 5.9. The *dihedral group* D_n is the group of symmetries of the regular n -gon (polygon with n sides).

Group? Now that we have defined permutation groups it is very easy to see that the dihedral groups are indeed groups. Observe that a symmetry of an n -gon can be viewed as a permutation of the corners of the n -gon for which ‘neighborliness’ is preserved. This is similar to how we viewed the Klein 4-group above.

For example, if we label the corners of the regular hexagon 1 through 6 then we see that D_6 is the set of $\sigma \in S_6$ such that $\sigma(1)$ is always next to $\sigma(6)$ and $\sigma(2)$, etc.

Clearly this says that $D_6 \subseteq S_6$.

To see that D_6 is a subgroup of S_6 , we need only note that the composition of two neighbor-preserving transforms must also preserves neighbors, as does the inverse of such a map.



Elements of D_n The regular n -gon has $2n$ distinct symmetries and so $|D_n| = 2n$. These consist of:

n rotations For each $j = 0, \dots, n - 1$, let ρ_j be rotation counter-clockwise by $\frac{2\pi j}{n}$ radians.

n reflections Let μ_j be reflection across the line making angle $\frac{\pi j}{n}$ with the positive x -axis (make sure you put one of the corners of the n -gon on the x -axis!).³

Remarks Some authors write D_{2n} instead of D_n precisely because $|D_n| = 2n$: in this course, D_n will *always* mean the symmetries of the n -gon.

Every dihedral group D_n is a subgroup of the orthogonal group $O_2(\mathbb{R})$. The correspondence is:

$$\rho_j = \begin{pmatrix} \cos\left(\frac{2\pi j}{n}\right) & -\sin\left(\frac{2\pi j}{n}\right) \\ \sin\left(\frac{2\pi j}{n}\right) & \cos\left(\frac{2\pi j}{n}\right) \end{pmatrix} \quad \mu_j = \begin{pmatrix} \cos\left(\frac{2\pi j}{n}\right) & \sin\left(\frac{2\pi j}{n}\right) \\ \sin\left(\frac{2\pi j}{n}\right) & -\cos\left(\frac{2\pi j}{n}\right) \end{pmatrix}$$

It is a good exercise to convince yourself that these matrices really do correspond to the rotations and reflections claimed. In particular multiply any two of them together and see what you get...

Subgroup relations between dihedral groups

$D_m \leq D_n \iff m \mid n$. Recall the discussion of geometric proofs earlier where we saw that $D_3 \leq D_6$. For instance, we can join every $(n/m)^{\text{th}}$ vertex of a regular n -gon to obtain a regular m -gon. Every symmetry of the m -gon is then a symmetry of the n -gon.

³For even-sided polygons these are often labelled differently, and split into two subsets of $\frac{n}{2}$ reflections each. The reflections μ_i are those which move *all* the corners of the n -gon, while δ_i refers to a reflection across a *diagonal*. We will see this in our treatment of D_4 below. In the abstract, it is simpler not to distinguish between these reflections.

Explicit descriptions of D_3 and D_4

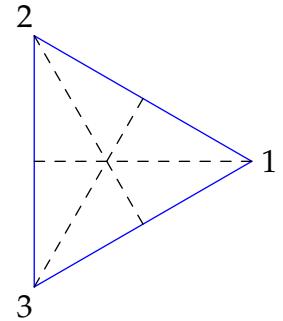
D_3 is the group of symmetries of an equilateral triangle. If we label the corners as in the picture, we can easily define the elements of the group.

ρ_0 the identity

ρ_1 rotate counter-clockwise by $\frac{2\pi}{3}$ radians

ρ_2 rotate clockwise by $\frac{2\pi}{3}$ radians

μ_i reflect in the altitude through i



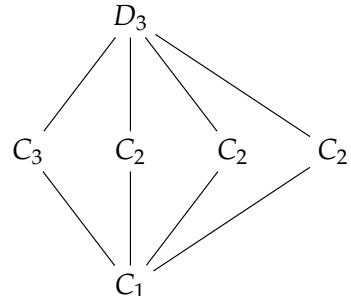
Here we write all the elements in permutation notation and give the Cayley table.

\circ	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

	Element	Standard notation	Cycle notation
Rotations	ρ_0	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$e = ()$
	ρ_1	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	(123)
	ρ_2	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	(132)
	μ_1	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	(23)
	μ_2	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	(13)
	μ_3	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	(12)

It should be immediately obvious that all the permutations of $\{1, 2, 3\}$ are elements of D_3 , and so $D_3 \cong S_3$. Now we consider all the subgroups of D_3 and its subgroup diagram.

Subgroup	Isomorph	Generating sets
$\{\rho_0\}$	C_1	$\{\rho_0\}$
$\{\rho_0, \mu_1\}$	C_2	$\{\mu_1\}$
$\{\rho_0, \mu_2\}$	C_2	$\{\mu_2\}$
$\{\rho_0, \mu_3\}$	C_2	$\{\mu_3\}$
$\{\rho_0, \rho_1, \rho_2\}$	C_3	$\{\rho_1\}$, or $\{\rho_2\}$
D_3	S_3	any pair $\{\rho_i, \mu_j\}$ where $i = 1, 2$ and $j = 1, 2, 3$



How can we be certain that there are no other subgroups of D_3 ? A careful consideration of generating sets should convince you. For example, suppose that a subgroup contains two reflections: WLOG suppose these are μ_1, μ_2 . We compute the subgroup generated by $\{\mu_1, \mu_2\}$. It must include

$$\mu_1\mu_2 = \rho_1, \quad \rho_1^2 = \rho_2 \quad \mu_1\rho_1 = \mu_3$$

and thus the entire group.

D_4 is the group of symmetries of the square. It consists of four rotations and four reflections: the notation δ_j for reflection across a diagonal is used here, rather than labelling all reflections μ_j .

ρ_0 the identity

ρ_1 rotate counter-clockwise by $\frac{\pi}{2}$ radians

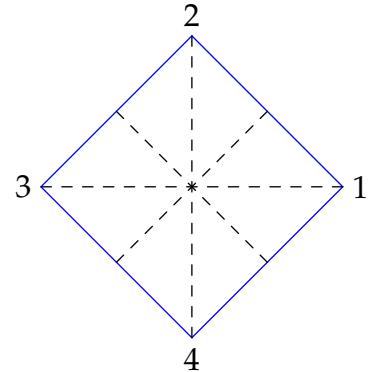
ρ_2 rotate counter-clockwise by π radians

ρ_3 rotate counter-clockwise by $\frac{3\pi}{2}$ radians

μ_i reflect across midpoints of sides

δ_i reflect across diagonals

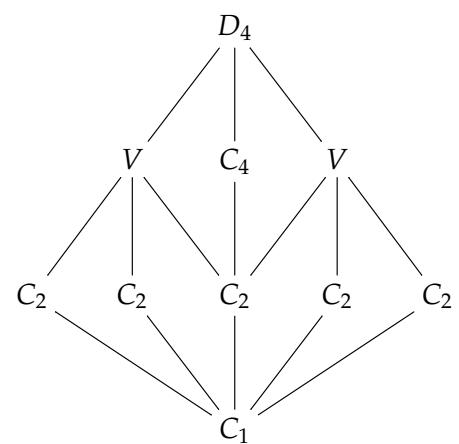
\circ	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_2	δ_1	μ_1	μ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_1	δ_2	μ_2	μ_1
μ_1	μ_1	δ_1	μ_2	δ_2	ρ_0	ρ_2	ρ_1	ρ_3
μ_2	μ_2	δ_2	μ_1	δ_1	ρ_2	ρ_0	ρ_3	ρ_1
δ_1	δ_1	μ_2	δ_2	μ_1	ρ_3	ρ_1	ρ_0	ρ_2
δ_2	δ_2	μ_1	δ_1	μ_2	ρ_1	ρ_3	ρ_2	ρ_0



Element	Standard notation	Cycle notation
ρ_0	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$	$e = ()$
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$	(1234)
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$	$(13)(24)$
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$	(1432)
μ_1	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$	$(12)(34)$
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$	$(14)(23)$
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$	(24)
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$	(13)

All the subgroups are summarised in the following table. In particular, note that $D_4 \not\cong S_4$: the latter has many more elements!

Subgroup	Isomorph	Generating sets
$\{\rho_0\}$	C_1	$\{\rho_0\}$
$\{\rho_0, \mu_i\}$	C_2	$\{\mu_i\}$ for each i
$\{\rho_0, \delta_i\}$	C_2	$\{\delta_i\}$ for each i
$\{\rho_0, \rho_2\}$	C_2	$\{\rho_2\}$
$\{\rho_0, \rho_1, \rho_2, \rho_3\}$	C_4	$\{\rho_1\}$ or $\{\rho_3\}$
$\{\rho_0, \mu_1, \mu_2, \rho_2\}$	V	$\{\mu_1, \mu_2\}$, $\{\mu_1, \rho_2\}$ or $\{\mu_2, \rho_2\}$
$\{\rho_0, \delta_1, \delta_2, \rho_2\}$	V	$\{\delta_1, \delta_2\}$, $\{\delta_1, \rho_2\}$ or $\{\delta_2, \rho_2\}$
D_4	D_4	any pair $\{\rho_i, \mu_j\}$ or $\{\rho_i, \delta_j\}$ where $i = 1, 3$ and $j = 1, 2$ or any pair $\{\mu_k, \delta_l\}$ where $k, l = 1, 2$



In the subgroup diagram, the middle C_2 is $\{\rho_0, \rho_2\}$ while the two copies on each side contain either the reflections δ_i or μ_i .

5.3 Orbits

In this section we continue the idea of a group being a set of permutations. In particular, we will see how any element $\sigma \in S_n$ partitions the set $\{1, 2, \dots, n\}$. This concept will be generalized later when we consider group actions.

Definition 5.10. The *orbit* of $\sigma \in S_n$ containing $j \in \{1, 2, \dots, n\}$ is the set

$$\text{orb}_j(\sigma) = \{\sigma^k(j) : k \in \mathbb{Z}\} \subseteq \{1, 2, \dots, n\}$$

Observe that $\text{orb}_{\sigma^k(j)}(\sigma) = \text{orb}_j(\sigma)$ for any $k \in \mathbb{Z}$.

Be careful: each orbit is a subset of the set $\{1, 2, \dots, n\}$, *not* of the group S_n .

Examples If $\sigma \in S_n$ is written in cycle notation (recall Definition 5.8) using *disjoint cycles*, then the cycles are the orbits! For example, in S_5 ,

Orbits of (134) are $\{1, 3, 4\}, \{2\}, \{5\}$

Orbits of $(12)(45)$ are $\{1, 2\}, \{3\}, \{4, 5\}$

The same does not hold if the cycles are not disjoint. For example, $\sigma = (13)(234) \in S_4$ maps

$$1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$$

so there is only one orbit: $\text{orb}_j(\sigma) = \{1, 2, 3, 4\}$ for any j . In fact, $\sigma = (1234)$, from which the orbit is obvious.

Given that disjoint cycle notation is so useful for reading orbits, it is a natural question to ask if *any* permutation σ can be written as a product of disjoint cycles. The answer, of course, is yes, with the disjoint cycles turning out to be precisely the orbits of σ !

Theorem 5.11. The orbits of any $\sigma \in S_n$ partition $X = \{1, 2, \dots, n\}$.

Proof. Define \sim on $X = \{1, 2, \dots, n\}$ by

$$x \sim y \iff y \in \text{orb}_x(\sigma)$$

We claim that \sim is an equivalence relation.

Reflexivity $x \sim x$ since $x = \sigma^0(x)$. ✓

Symmetry $x \sim y \implies y = \sigma^k(x)$ for some $k \in \mathbb{Z}$. But then $x = \sigma^{-k}(y) \implies y \sim x$. ✓

Transitivity Suppose that $x \sim y$ and $y \sim z$. Then $y = \sigma^k(x)$ and $z = \sigma^l(y)$ for some $k, l \in \mathbb{Z}$. But then $z = \sigma^{k+l}(x)$ and so $x \sim z$. ✓

The equivalence classes of \sim are clearly the orbits of σ , which therefore partition X . ■

Corollary 5.12. Every permutation can be written as a product of disjoint cycles.

Proof. Write out each of the orbits of $\sigma \in S_n$ in order, placing each orbit in parentheses (). Since the orbits of σ partition $X = \{1, 2, \dots, n\}$ the cycles obtained are disjoint.

More concretely,

$$\text{orb}_1(\sigma) = \{1, \sigma(1), \sigma^2(1), \dots\}$$

If this orbit is the entirity of X , then we are finished. Otherwise, let

$$x_1 = \min\{x : x \notin \text{orb}_1(\sigma)\}$$

and construct its orbit:

$$\text{orb}_{x_1}(\sigma) = \{x_1, \sigma(x_1), \sigma^2(x_1), \dots\}$$

This orbit must be disjoint with $\text{orb}_1(\sigma)$. Now repeat. It is immediate from the construction that

$$\sigma = (1 \ \sigma(1) \ \sigma^2(1) \ \dots) (x_1 \ \sigma(x_1) \ \sigma^2(x_1) \ \dots) (\dots \dots)$$

■

Examples If you mechanically follow the algorithm for multiplying cycles (see the previous section) you will automatically end up with a product of disjoint cycles:

1. $(13)(234)(1432) = (123)$
2. $(13)(24)(12)(34) = (14)(23)$

Note that disjoint cycles commute! E.g. $(14)(23) = (23)(14)$.

Now that we are able to write any permutation as a product of disjoint cycles, we are able to compute much more easily. For example:

Theorem 5.13. *The order of a permutation σ is the least common multiple of the lengths of its disjoint cycles.*

Proof. Write σ as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_m$. Since disjoint cycles commute, it is immediate that

$$\sigma^n = \sigma_1^n \cdots \sigma_m^n$$

Moreover, since the terms σ_j^n permute disjoint sets, it follows that

$$\sigma^n = e \iff \forall j, \sigma_j^n = e$$

A k -cycle clearly has order k (the least positive integer l such that $(a_1 \cdots a_k)^l = e$). If the orbits of σ have lengths $\alpha_j \in \mathbb{N}$ respectively, it follows that

$$\sigma_j^n = e \iff \alpha_j \mid n$$

Thus n must be a multiple of α_j for all j . The least such n is clearly $\text{lcm}\{\alpha_j\}$.

■

Example The order of $\sigma = (145)(3627)(89) \in S_9$ is $\text{lcm}(3, 4, 2) = 12$.

We can easily calculate σ^{3465} for the above σ . Since $3465 = 12 \cdot 288 + 9$ we have

$$\sigma^{3465} = (\sigma^{12})^{288}\sigma^9 = \sigma^9 = (145)^9(3627)^9(89)^9 = (3627)(89)$$

since (145) , (3627) and (89) have orders 3, 4 and 2 respectively.

5.4 Transpositions

Instead of breaking a permutation σ into disjoint cycles, we can consider a permutation as being constructed from only the simplest bijections.

Definition 5.14. A 2-cycle (a_1a_2) is also known as a *transposition*, since it swaps two elements of $\{1, 2, \dots, n\}$ and leaves the rest untouched.

Theorem 5.15. Every $\sigma \in S_n$ is the product of transpositions.

Proof. There are many, many ways to write out a single permutation as a product of transpositions. One method is to first write σ as a product of disjoint cycles, then write each cycle as follows:

$$(a_1 \dots a_k) = (a_1a_k)(a_1a_{k-1}) \dots (a_1a_2)$$

Just look carefully to see that this works! ■

Example $(17645) = (15)(14)(16)(17)$

Definition 5.16. A permutation $\sigma \in S_n$ is *even/odd* if it can be written as the product of an even/odd number of transpositions.

Theorem 5.17. The concepts of even/odd are well-defined: every permutation is either even or odd, and not both.

Proof. Recall that any permutation $\sigma \in S_n$ can be written as an $n \times n$ permutation matrix (Definition 5.6). A 2-cycle is a permutation matrix which swaps two rows: it therefore differs from the $n \times n$ identity matrix only in that two of its rows are swapped. For example

$$(24) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in S_4$$

From linear algebra we have that swapping two rows of a matrix changes the sign of its determinant. Hence $\det(2\text{-cycle}) = -1$. It follows that

$$\det(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is the product of an even number of 2-cycles,} \\ -1 & \text{if } \sigma \text{ is the product of an odd number of 2-cycles.} \end{cases}$$

In particular σ cannot be both odd and even. ■

5.5 The Alternating Groups

The concept of even permutations leads us to the definition of a new collection of groups.

Definition 5.18. The alternating group A_n ($n \geq 2$) is the group of even permutations in S_n .

Theorem 5.19. A_n has exactly half the elements of S_n : that is $|A_n| = \frac{n!}{2}$.

Proof. Since $n \geq 2$, we have $(12) \in S_n$. Define $\phi : A_n \rightarrow \{\text{odd permutations}\}$ by $\phi(\sigma) = (12)\sigma$. We claim that this is a bijection

$$1-1 \quad \phi(\sigma) = \phi(\tau) \implies (12)\sigma = (12)\tau \implies \sigma\tau. \checkmark$$

Onto If ρ is an odd permutation, then $(12)\rho$ is even and so in A_n . Therefore $\rho = \phi((12)\rho)$. \checkmark

Since ϕ is a bijection, it follows that there are exactly the same number of even and odd permutations in S_n . Exactly half of them are therefore even. \blacksquare

Examples: small alternating groups

1. $A_2 = \{e\}$ is extremely boring!
2. $A_3 = \{e, (13)(12), (12)(13)\} = \{e, (123), (132)\}$ is simply the cyclic group of order 3.
3. $A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$ is the first genuinely new group in the alternating family. It has order 12 and is non-Abelian: for example

$$(123)(124) = (13)(24) \neq (14)(23) = (124)(123)$$

We already know of one non-Abelian group of order 12: the dihedral group D_6 . But we can quickly see that A_4 is non-isomorphic to D_6 : all elements of A_4 have order 1, 2 or 3, while D_6 , being the symmetries of a hexagon, contains a rotation of order 6.

A concrete appearance of A_4 can be seen as the group of rotations of a tetrahedron. Either label the corners of a tetrahedron, or the faces, with the numbers 1, 2, 3, 4. Can you visualize how each element of A_4 transforms each tetrahedron?

