1 Permutation groups and group actions

1.1 What is a permutation and how does one present it

- **Definition of a permutation**: A *permutation of a set* Ω is a bijective mapping from Ω onto itself.

- **Tabular form of a permutation**: We may write a permutation in tabular form. For example:

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

  meaning 1 maps to 3, 2 to 6, 3 to 5, etc.

- **Cyclic form of a permutation**: But usually we write a permutation as a *product of disjoint cycles* or *in a cyclic form*. For example:

$$g = (1,3,5)(2,6)(4) = (5,1,3)(2,6)(4) = (3,5,1)(6,2)(4) = \dots$$

  where g is as abve.

- **Cycles of a permutation**: The sequences $(1,3,5)$, $(2,6)$ and (4) of the above g are called the *cycles of the permutation* g. The above g thus consists of one cycle of length 3, one cycle of length 2 and one cycle of length 1.

- **Cyclic permutation**: A permutation that has only one cycle of length larger than 1 is called a *cyclic permutation* (or also a *cycle*).

- **Omitting cycles of length 1**: When presenting a permutation, we sometimes omit cycles of length 1. We could thus write the above g also as

$$g = (1,3,5)(2,6).$$

- **The set of all permutations**: The set of all permutations of Ω is denoted by $\mathrm{Sym}(\Omega)$.

- **Exponential notation**: Henceforth, if $\omega \in \Omega$ and $g \in \mathrm{Sym}(\Omega)$, then we write the image of ω under g as ω^g, rather than $g(\omega)$.

1.2 Multiplying permutions and the symmetric group

- **Composition of permutations**: Since permutations on Ω are function from Ω to Ω, we have a naturally defined operation of the usual *composition* of functions.

- **Example of composition**: If $\Omega = \{1, 2, 3, 4, 5\}$, $g = (1, 3, 4)(2, 5)$ and $h = (2, 4, 5)$, then

$$g \circ h = (1, 3, 4, 2) \quad \text{and} \quad h \circ g = (1, 3, 5, 4).$$

- **Left symmetric group**: The operation $\circ$ turns the set $\mathrm{Sym}(\Omega)$ into a group, which will be denoted $\mathrm{Sym}_L(\Omega)$.

- **Inverse composition**: But we shall rather work with the operation of *inverse composition* defined as:

$$\cdot : \mathrm{Sym}(\Omega) \times \mathrm{Sym}(\Omega) \to \Omega, \qquad \cdot : (g, h) \mapsto h \circ g.$$

- **Composition vs. inverse composition**: Note that

$$g \circ h = h \cdot g$$

  and that

$$\omega^{(g \cdot h)} = (\omega^g)^h \quad \text{while} \quad \omega^{(g \circ h)} = (\omega^h)^g.$$

  for every $\omega \in \Omega$ and $g, h \in \mathrm{Sym}(\Omega)$.

- **The right symmetric group**: The operation of inverse composition also turns the set $\mathrm{Sym}(\Omega)$ into a group, which we will denote $\mathrm{Sym}_R(\Omega)$.

- **Our heart is on the right**: Henceforth, we shall always work with $\mathrm{Sym}_R(\Omega)$. We will often omit the symbols R, call the inverse composition the *product of permutations*. As usual in group theory, we shall also omit the symbol $\cdot$ and write gh instead of $g \cdot h$.

- **Transpositions and what they generate**: A permutation of the form (α, β) is called a *transposition*. Each permutation can be written as a product of transpositions. In other words, the set of all transpositions on Ω *generates* $\mathrm{Sym}(\Omega)$

- **Even and odd permutations**: If g can be written as a product of an *odd* number of transposition, then it cannot we written as a product of *even* number of transpositions and vice versa. This allows as to define the notion of *odd permutation* and *even permutation*. The set of all even permutations of Ω forms a subgroup of $\mathrm{Sym}(\Omega)$, which will be denoted by $\mathrm{Alt}(\Omega)$.

1.3 Examples of permutation groups

We shall use the symbol $[n]$ to denote the set of positive integers not exceeding n.

- Alternating groups: $\mathrm{Alt}(\Omega) =$ "the set of all even permutations on Ω";
- Cyclic groups: $\mathrm{Cyc}(n) = \langle(1, 2, \dots, n)\rangle$ with $\Omega = [n]$;
- Dihedral groups: $\mathrm{Dih}(n) = \langle(1, 2, \dots, n),(1)(2, n - 1)(3, n - 2)\cdots\rangle$ with $\Omega = [n]$
- Groups of affine transformations of a ring: For a commutative ring R with identity, let $\mathrm{Aff}(R) = \{x \mapsto ax + b : a \in R^*, b \in R\}$; then this is a permutation group on the set R. Note that $|\mathrm{Aff}(R) = |R|\,|R^*|$. For example: $\mathrm{Aff}(\mathbb{Z}_3) = \mathrm{Sym}(\mathbb{Z}_3)$.
- The projective special group $\mathrm{PSL}(2, q)$: Let $\mathbb{F}$ be a field of prime power order q and let $\mathrm{PGL}(2, q) = \{x \mapsto \frac{ax+b}{cx+d} : a, c \in \mathbb{F}^*, b, d \in R, ad - bcnot = 0\}$ as a permutation group on $\mathbb{F} \cup \{\infty\}$. Here we interpret $\frac{a\infty+b}{c\infty+d}$ as ac^{-1} and $\frac{k}{0}$ for $k \neq 0$ as ∞.
- The subgroup of $\mathrm{PGL}(2, q)$ consisting of functions satisfying $ad-bc = 1$, is denoted $\mathrm{PSL}(2, q)$.

1.4 Exercises

Exercise.

1. Find the cyclic form of the permutation $g\colon \Omega \to \Omega$ given by:

   (a) $\Omega = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 4 & 8 & 5 & 1 & 6 \end{pmatrix},$$

(b) $\Omega = \mathbb{Z}_7$, the ring of remainders after division by 7, and $g(x) = 2x + 1$. (Which "linear functions" $h\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $h_{a,b}(x) = ax + b$, are permutions, how many cycles do they have and what are the lengths?)

2. Show that $\mathrm{Sym}_L(\Omega)$ and $\mathrm{Sym}_R(\Omega)$ are isomorphic.
3. Let Ω and Δ be two sets of equal cardinality. Show that $\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(\Delta)$.
4. Let the lengths of cycles of g be $d_1, d_2, \ldots, d_k$. What is the order of g? (Recall that the order of a group element g is the smallest positive integer m such that $g^m = \mathrm{id}$).
5. If $g, h \in \mathrm{Sym}(\Omega)$, then we call the product $g^{-1}hg$ a *conjugate* of h (by g) and write it as h^g. Compute h^g for $h = (1, 2, 3)(4, 5)(6, 7)$ and

   - $g = (0, 1, 2, 3, 4, 5, 6, 7)$,
   - $g = (1, 2)$,
   - $g = (1, 2)(4, 5)$.

   What is the general pattern for computing conjugates?
6. Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$ and $g = (\omega_1, \omega_2, \ldots, \omega_n)$ a cyclic permutation on Ω. Determine the centraliser and the normaliser of the cyclic group $\langle g \rangle$ generated by g.
7. Show that two permutations $g, h \in \mathrm{Sym}(\Omega)$ are conjugate in $\mathrm{Sym}(\Omega)$ whenever they have the same number of cycles of length k for every possible cycle length k.
8. Determine the order of $\mathrm{PSL}(2, q)$. To which well known groups are $\mathrm{PSL}(2, 2)$, $\mathrm{PSL}(2, 3)$, $\mathrm{PSL}(2, 4)$ and $\mathrm{PSL}(2, 5)$ isomorphic to? Find the corresponding isomorphisms.