1.3 Properties of permutations

Proposition 1.3.1. *Taking products of permutations is associative; i.e.* $(\sigma\rho)\tau = \sigma(\rho\tau)$.

Proof. Composition of functions is associative, and so it follows immediately that composition of bijective functions (i.e. products of permutations) is also associative. □

Definition 1.3.2. Let X be any set. The *identity permutation* in $\mathrm{Sym}(X)$ is the permutation that fixes every element in X. It is denoted by e (or sometimes Id).

Proposition 1.3.3. *Let X be any set. The following hold for all $\sigma, \rho \in \mathrm{Sym}(X)$.*

(i) $\sigma e = e\sigma = \sigma$

(ii) The product $\sigma\rho$ is also a permutation in $\mathrm{Sym}(X)$

(iii) There exists an inverse permutation $\sigma^{-1} \in \mathrm{Sym}(X)$ such that $\sigma^{-1}\sigma = e$.

Proof. (i) Easy exercise.
(ii) The composition of two bijections is still a bijection.
(iii) Every bijection $f : X \to Y$ is known to have an inverse $f^{-1} : X \to Y$ such that $f^{-1} \circ f(x) = x$ for all $x \in X$. One can easily see that f^{-1} must also be a bijection.
Since σ is a bijection, we can apply this fact to σ to find σ^{-1}. Since $\sigma^{-1}\sigma x = x$ for all $x \in X$ we know that $\sigma^{-1}\sigma = e$. □

Notation. For $\sigma \in \mathrm{Sym}(X)$ and $n \in \mathbb{N}$ we write σ^n to mean $\sigma \circ \sigma \circ \cdots \circ \sigma$ (n times), and σ^{-n} to mean $\sigma^{-1} \circ \sigma^{-1} \circ \cdots \circ \sigma^{-1}$ (n times). We also define σ^0 to be e. It is easy to check that all the usual rules (e.g. $\sigma^n\sigma^m = \sigma^{n+m}$) apply.

Proposition 1.3.4. *Let X be a finite set. Every permutation in* $\mathrm{Sym}(X)$ *can be written as a product of disjoint cycles.*

The following result allows us to find inverses of permutations quickly when they are written in cycle notation.

Proposition 1.3.5. (Quick Inverse Proposition). *Let X be a set and suppose $\sigma \in \mathrm{Sym}(X)$. We know (from previous result) that we can write σ as a product of disjoint cycles:*

$$\sigma = c_1 c_2 \cdots c_n.$$

Then

(i) The inverse of any cycle $(x_1\ x_2\ \ldots\ x_m)$ is $(x_m\ x_{n-1}\ \ldots x_1)$, and

(ii) $\sigma^{-1} = c_1^{-1} c_2^{-1} \ldots c_n^{-1}$.

Proof. To prove (i) is easy: just calculate $(x_1\ x_2\ \ldots\ x_m)(x_m\ x_{m-1}\ \ldots x_1)$ and note that it is equal to $(x_1)(x_2)\cdots(x_m) = e$.
To prove (ii) we recall that by Proposition 1.2.7, disjoint cycles commute. Now the cycles $c_1^{-1}, c_2^{-1}, \ldots, c_n^{-1}$ are disjoint, therefore:

$$c_1^{-1}c_2^{-1}\cdots c_n^{-1}\sigma = c_1^{-1}c_2^{-1}\cdots c_n^{-1}c_1c_2\ldots c_n = c_2^{-1}\cdots c_n^{-1}c_1^{-1}c_1c_2\ldots c_n = c_2^{-1}\cdots c_n^{-1}ec_2\ldots c_n = \cdots = e.$$

□

Example 1.3.6. Find the inverse of $(1\,5\,7)(2\,3\,8)$. It is $(7\,5\,1)(8\,3\,2)$.

Definition 1.3.7. The order of a permutaion $g \in \mathrm{Sym}(X)$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$ if such an n exists; if not then the order of g is infinite. The order of g is denoted by $o(g)$.

Conclusion: We have shown that $\mathrm{Sym}(X)$ has the following properties:

- It has an identity e and the product of two elements in $\mathrm{Sym}(X)$ still lies in $\mathrm{Sym}(X)$
- Every element has an inverse in $\mathrm{Sym}(X)$ and the product is associative

1.3.1 Handout for Section 1.3

The object $\mathrm{Sym}(X)$ was studied in the 18th Century (by Lagrange) as a means of finding solutions to polynomials (by radicals). Later Galois called this object a group.
Independently (and slightly later), in geometry and in number theory, mathematicians were studying other objects with these properties. Eventually (in the 1870s with Camille Jordan) any object satisfying these four axioms came to be known as a group.
Groups of permutations were the first groups to be studied, and (as we shall see with Cayley's Theorem later) every group can be thought of as a permutation group.

Proof of Proposition 1.3.4. Fix $\sigma \in \mathrm{Sym}(X)$. Let's write X as $\{x_1, \ldots, x_n\}$. Consider the list

$$\sigma^0 x_1, \quad \sigma^1 x_1, \quad \sigma^2 x_1, \quad \sigma^3 x_1, \quad \ldots.$$

Since X is finite, we must eventually get a repetition. Say $\sigma^a x_1$ is the first repeat. Then $\sigma^a x_1 = \sigma^b x_1$ for some $0 \leq b \leq a-1$. Hence

$$\sigma^a x_1 = \sigma^b x_1, \qquad \text{therefore} \qquad \sigma^{-b}\sigma^a x_1 = \sigma^{-b}\sigma^b x_1.$$

Hence $\sigma^{a-b} x_1 = x_1$, but the first repeat was a, therefore $b = 0$. Hence,

$$\sigma^a x_1 = x_1.$$

Let c_1 be the cycle

$$c_1 = (x_1 \quad \sigma x_1 \quad \sigma^2 x_1 \quad \ldots \quad \sigma^{a-1} x_1)$$

and note that σ and c_1 agree on all the symbols in c_1.
Now let k be the smallest number such that x_k is not listed inside c_1. Now list

$$\sigma^0 x_k, \quad \sigma^1 x_k, \quad \sigma^2 x_k, \quad \sigma^3 x_k, \quad \ldots,$$

Again there will be a first repeat $\sigma^d x_k$ and by the above argument we will have $x_k^d = x_k$. Let c_2 be the cycle

$$c_2 = (x_k \quad \sigma x_k \quad \sigma^2 x_k \quad \ldots \quad \sigma^{d-1} x_k).$$

We claim that the two cycles are disjoint. Proof of claim: if $\sigma^i x_1 = \sigma^j x_k$ then $x_k = \sigma^{i-j} x_1$, which contradicts our assumption that x_k does not lie in c_1. Hence our claim is true.
Now $c_1 c_2$ agrees with σ on all the symbols in c_1 and c_2. We can repeat the above process to find cycles c_3, $\ldots$, c_ℓ that are all disjoint such that $c_1 c_2 \cdots c_\ell$ and σ agree on X. Since they agree on X, they are the same permutation of X, and we have thus written σ as a product of disjoint cycles. □

Remark 1.3.8. A similar argument can be used to show the above holds if X is countably infinite, which would strengthen Proposition 1.3.4. Can you see how?

1.4 Exercises 1- Exercises on permutations

(S)

Question 1.4.1. (a) Write the following permutation as a product of disjoint cycles:

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 7 & 2 & 1 & 5 & 6 & 3 \end{array}$$

(b) Write the following permutation as a product of disjoint cycles:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 1 & 4 & 2 \end{array}$$

(c) Write the following permutation out in full (using the above arrow notation):

$$(1\ 7\ 2\ 11\ 9)(4\ 10\ 5)(3\ 8\ 6) \in S_{12}$$

Question 1.4.2. Let $g = (1\ 4\ 2\ 7\ 8)$, $h = (1\ 4\ 5)$ and $k = (5\ 7\ 9)(1\ 3\ 2)$. Write the following as a product of disjoint cycles.

(a) k^{-1} (Check your answer by calculating kk^{-1})

(b) ghk

(c) $k^{-1}ghk$

Question 1.4.3. The *order* of a permutation σ is written $o(\sigma)$, and is defined to be the smallest natural number $n \geq 1$ such that $\sigma^n = e$. E.g. $o((1\ 2\ 3)) = 3$ and $o(e) = 1$. We will discuss the order of group elements in more detail later in the course, but for now try to answer the following questions.

(a) What is the order of the permutation $(1\ 2\ 3\ 4\ 5)$?

(b) What is the order of the permutation $(1\ 5\ 7)(2\ 3\ 6)$?

(c) What is the order of the permutation $(1\ 3\ 5)(2\ 4)$?

(d) Find an element of S_{10} with order 15.

(e) Is there an element of S_{10} with order 19? If so, find it; if not, why not?

(f) Suppose a permutation $g \in S_n$ is written as a product of disjoint r_i-cycles,

$$g = c_1 c_2 \cdots c_m.$$

Can you find a formula to calculate $o(g)$? Can you prove your formula is correct?
[Hint: first try to work out a formula for the order of a cycle of length r_i.]

Question 1.4.4. Find a permutation $\sigma \in S_4$ that satisfies the following permutation equation:

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

Question 1.4.5. Find a permutation $\sigma \in S_7$ that satisfies the following permutation equation:

$$(1\ 3\ 2)(5\ 7\ 4)\sigma = (1\ 2)(3\ 4)$$

Question 1.4.6. Find a permutation $\sigma \in S_9$ that satisfies the following permutation equation:

$$(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9)\sigma = (9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1)$$

2 Groups

2.1 An recap of groups

Definition 2.1.1. A *group* is a set G together with an operation $*$ on G such that each of the following holds.

(i) **Closure**: for all $g, h \in G$,
$$g * h \in G.$$

(ii) **Existence of an identity element**: $\exists e_G \in G$ such that for all $g \in G$,
$$g * e_G = e_G * g = g.$$

(iii) **Existence of inverse elements**: For all $g \in G$ there exists an inverse element $g^{-1} \in G$ such that
$$g * g^{-1} = g^{-1} * g = e_G.$$

(iv) **Associativity**: for all $g, h, k \in G$,
$$g * (h * k) = (g * h) * k$$

We don't usually bother writing the operation symbol, so $g * h$ will usually be written as gh.
By definition, $g^0 := e_G$ for all $g \in G$.
A *subgroup* H of a group G is a subset of G that is also a group under the operation of G. Write $H \leq G$ when H is a subgroup of G. So for example $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$ but $(\mathbb{Q}^*, \times) \not\leq (\mathbb{R}, +)$.

Example 2.1.2. (Very important) Let X be a set and let $\mathrm{Sym}(X)$ be the collection of all permutations of X under the operation of permutation multiplication (as described in the previous section).
As we have seen, $\mathrm{Sym}(X)$ satisfies the group axioms and is therefore a group. It is called the *symmetric group on* X and is an example of a *permutation group*.

Definition 2.1.3. If G and H are groups, then their direct product (also called Cartesian product) $G \times H$ is also a group, where $G \times H$ is the set $\{(g, h) \mid g \in G, h \in H\}$ with operation
$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

You proved this was a group in Algebraic Structures. Quick exercise: what is the identity of $G \times H$?

Definition 2.1.4. A group G is *abelian* if the group operation is commutative, that is
$$ab = ba$$
for all $a, b \in G$.

Warning! Most groups are not abelian!

Example 2.1.5. The groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}^*, \times)$ are abelian because addition and multiplication of numbers is commutative.

Non-Example 2.1.6. The group $\mathrm{GL}(2, \mathbb{R})$ is not abelian. Proof:
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 7 & 10 \end{pmatrix} \neq \begin{pmatrix} 7 & 10 \\ 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Definition 2.1.7. The *order* of a group G is the number of elements in G, and is denoted by $|G|$.

Definition 2.1.8. The order of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e_G$ if such an n exists; if not then the order of g is infinite. The order of g is denoted by $o(g)$.

2.1.1 Handout for Section 2.1

Example 2.1.9. Here are some examples of groups. All but the first example should be familiar to you.

(i) Let ξ be the set:

$$\xi = \{\heartsuit, 🚲\}$$

We define an operation $*$ on ξ as follows:

$$\heartsuit * \heartsuit = \heartsuit \quad \text{and} \quad \heartsuit * 🚲 = 🚲$$
$$🚲 * \heartsuit = 🚲 \quad \text{and} \quad 🚲 * 🚲 = \heartsuit$$

Then $(\xi, *)$ is a group (you should check this!).

(ii) The integers under addition: $(\mathbb{Z}, +)$. This group is sometimes abbreviated to $\mathbb{Z}$.

(Here $n * m = n + m$ for all $n, m \in \mathbb{Z}$)

(iii) Let $\mathbb{Q}^*$ be the set $\mathbb{Q} \setminus \{0\}$. Then $(\mathbb{Q}^*, \times)$ is a group.

(Here $a * b = a \times b$ for all $a, b \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$)

(iv) The set of invertible 2×2 matrices whose entries are real numbers is a group under matrix multiplication. This group is denoted by $\mathrm{GL}(2, \mathbb{R})$ and is called *the General Linear Group of* 2×2 *matrices over* $\mathbb{R}$. (The fact that this is a group was proved in Algebraic Structures.)

(Here $A * B$ means matrix multiplication, for all $A, B \in \mathrm{GL}(2, \mathbb{R})$)

Non-Example 2.1.10. Here are some examples of things that are **not** groups.

(i) The **set** $\mathbb{R}$
(not a group because no operation has been specified)

(ii) The natural numbers under addition $(\mathbb{N}, +)$
(not a group because some elements do not have inverses)

(iii) $(\mathbb{Q}^*, +)$
(not a group because it is not closed and has no inverse)

(iv) The set of all 2×2 matrices whose entries are real numbers is not a group under matrix multiplication
(not a group because some elements have no inverse)

Theorem 2.1.11. *Let G be a group and let $g \in G$.*

(i) *G has only one identity*

(ii) *g has only one inverse*

(iii) $(g^{-1})^{-1} = g$

(iv) *Let $h_1, h_2 \in G$. If $gh_1 = gh_2$ or $h_1 g = h_2 g$ then $h_1 = h_2$*

Warning! If $gh_1 = h_2 g$ it is **not necessarily** true that $h_1 = h_2$

(v) $(h_1 h_2)^{-1} = h_2^{-1} h_1^{-1}$

(vi) $(g^n)^{-1} = g^{-n}$

Proof. These facts were all proved in Algebraic Structures. Prove them again if you want to as an exercise. □