2.1 A little bit about functions

Lemma 2.1.2: Associativity of function composition ∘ (p40)

Let A, B, C and D be sets and let $h : A \to B$, $g : B \to C$ and $f : C \to D$ be functions. Then

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Injectivity

A function $f : A \to B$ is called **injective** if and only if

$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \quad \iff \quad \forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

Surjectivity

A function $f : A \to B$ is called **surjective** if and only if

$$\forall b \in B : \exists a \in A : f(a) = b$$

Bijectivity

A function $f : A \to B$ is called **bijective** if and only if it is both injective and surjective.

$$\begin{aligned} f \text{ is bijective} &\iff f \text{ is injective and } f \text{ is surjective} \\ &\iff \forall b \in B : \exists! a \in A : f(a) = b \end{aligned}$$

Definition 2.1.3: Inverse Function (p42)

Let $f : A \to B$ be a function. A function $g : B \to A$ is called *the* **inverse** of f if

$$f \circ g = id_B \quad \text{and} \quad g \circ f = id_A$$

We denote the inverse of f by f^{-1}.

Lemma 2.1.4: A function is invertible if and only if it is bijective (p43)

Let $f : A \to B$ be a function.

$$f \text{ is bijective} \iff f \text{ is invertible}$$

Lemma 2.1.5: About cardinalities of the domain and codomain of functions (p43)

Suppose that A and B are sets and let $f : A \to B$ be a function.

- If f is injective, then $|A| \leq |B|$.
- If f is surjective, then $|A| \geq |B|$.

Lemma 2.1.6 (p44)

Let A and B be finite sets with $|A| = |B|$ and let $f : A \to B$ be a function.

- If f is injective, then f is bijective.
- If f is surjective, then f is bijective.

2.2 Definition of permutations

Permutation (p44)

A **permutation** of a set A is a **bijective** function $f: A \to A$.

Definition 2.2.1: Set of permutations (p45)

Let A be a set. The set of all permutations $f: A \to A$ is denoted by S_A.
In case $A = \{1, 2, \ldots, n\}$ we write S_n instead of $S_{\{1,2,\ldots,n\}}$.

We can write down a permutation $f \in S_n$ in two-line notation as

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f[a_1] & f[a_2] & \cdots & f[a_n] \end{pmatrix}$$

Composition of permutations (p46)

If we have two permutations f and g on the **same** set A, then we can compose them to get a new **permutation** $f \circ g$ **on** A:

$$(f \circ g)[a] := f[g[a]]$$

Proof
To see that $f \circ g$ is a *function from* A *to* A, we note that since g is a function from A to A, for every $a \in A$, $g[a]$ is well-defined and belongs to A. Then, since f is also a function from A to A, applying f to $g[a]$ gives us $(f \circ g)[a] = f[g[a]]$, which is also in A. Thus, for every $a \in A$, $(f \circ g)[a]$ is well-defined and belongs to A, confirming that $f \circ g$ is indeed a function from A to A.

To see that $f \circ g$ is *bijective*, we can use Lemma 2.1.4: since both f and g are **bijective**, they both have inverses, denoted by f^{-1} and g^{-1}. We can then check that

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = id_A \quad \text{and} \quad (g^{-1} \circ f^{-1}) \circ (f \circ g) = id_A$$

which shows that $f \circ g$ has an inverse

$$(f \circ g)^{-1} = (g^{-1} \circ f^{-1}),$$

and from Lemma 2.1.4 it follows that $f \circ g$ is indeed bijective.

Since a bijective function from a set to itself is a permutation, we conclude that $f \circ g$ is indeed a permutation on A.

Composing a permutation with itself (p47)

If f is a permutation on a set A, then we denote:

- $f^0 := id_A$
- $f^2 := f \circ f$
- ...
- $f^k := \underbrace{f \circ f \circ \cdots \circ f}_{k \text{ times}}$

Order of a permutation (p47)

Let f be a permutation on a set A. The **order** of f is defined as:

$$\operatorname{ord}(f) = \text{the smallest } i \in \mathbb{Z}_{\geq 0} \text{ such that } f^i = id_A$$

If no such i exists, then we say that f has **infinite order** and write

$$\operatorname{ord}(f) = \infty.$$

Theorem 2.2.7: Central properties of composition of permutations (p47-48)

Let A be a set and S_A the set of permutations on A. Further denote by $\circ$ the composition of permutations on S_A. Then we have:

1. The composition map is associative:
$$\forall f, g, h \in S_A : (f \circ g) \circ h = f \circ (g \circ h)$$
2. The identity permutation satisfies:
$$\forall f \in S_A : f \circ id_A = id_A \circ f = f$$
3. There exists an inverse for every permutation f, denoted by f^{-1}:
$$\forall f \in S_A : \exists g \in S_A : g \circ f = f \circ g = id_A$$

Definition 2.2.8: Symmetric group on A and on n letters (p48)

The pair $(S_A, \circ)$ is called the **symmetric group** on the set A.
In case $A = \{1, 2, \ldots, n\}$, we say that $(S_n, \circ)$ is the **symmetric group on n letters**.

2.3 Cycle notation

m-cycle (p48)

Let $m \geq 1$ be an integer. A permutation $f \in S_A$ is called an m**-cycle** if there exist m distinct elements $a_0, a_1, \ldots, a_{m-1} \in A$ such that

$$\begin{cases} f[a_i] = a_{(i+1) \bmod m} & \text{for } i = 0, 1, \ldots, m-1 \\ f[x] = x & \text{for all } x \in A \setminus \{a_0, a_1, \ldots, a_{m-1}\} \end{cases}$$

That is to say,

$$f[a_0] = a_1, \quad f[a_1] = a_2, \quad \ldots, \quad f[a_{m-2}] = a_{m-1}, \quad f[a_{m-1}] = a_0$$

and f leaves all elements in $A \setminus \{a_0, a_1, \ldots, a_{m-1}\}$ fixed.

Cycle notation (p49)

If f is an m-cycle as in the definition above, then we write f in **cycle notation** as

$$f = (a_0 \, a_1 \, a_2 \, \ldots \, a_{m-1})$$

Lemma 2.3.2: An m-cycle has order m (p49)

Let $m \geq 1$ be an integer and let $a_0, a_1, \ldots, a_{m-1}$ be distinct elements of A. Then the m**-cycle** $(a_0 \, a_1 \, a_2 \, \ldots \, a_{m-1})$ **has order m.**

Mutually disjoint cycles (p49)

Two cycles $(a_0 \, a_1 \, \ldots \, a_{m-1})$ and $(b_0 \, b_1 \, \ldots \, b_{k-1})$ are **mutually disjoint** if

$$\{a_0, a_1, \ldots, a_{m-1}\} \cap \{b_0, b_1, \ldots, b_{k-1}\} = \emptyset$$

Commuting permutations

Two permutations f and g on a set A are said to **commute** if

$$f \circ g = g \circ f$$

Disjoint cycles always commute

Let f and g be two permutations on a set A. If f and g are **mutually disjoint** cycles, then they commute:

$$f \circ g = g \circ f \quad \text{if } f \text{ and } g \text{ are disjoint cycles}$$

Proof

Let $f = (a_0\, a_1\, \dots\, a_{m-1})$ and $g = (b_0\, b_1\, \dots\, b_{k-1})$ be two mutually disjoint cycles on a set A. We want to show that $f \circ g = g \circ f$. This means that

$$\{a_0, a_1, \dots, a_{m-1}\} \cap \{b_0, b_1, \dots, b_{k-1}\} = \emptyset \quad \Longleftrightarrow \quad A \cap B = \emptyset$$

We will show that for every element $x \in A$, $(f \circ g)[x] = (g \circ f)[x]$.

We consider three cases based on the position of x:

1. **Case 1:** $x \in A \Leftrightarrow x \notin B$
   - If $x \in A$, then $g[x] = x$ (since g leaves elements outside its cycle fixed). Therefore,

     $$(f \circ g)[x] = f[g[x]] = f[x]$$

     and

     $$(g \circ f)[x] = g[f[x]] = f[x]$$

     Thus, $(f \circ g)[x] = (g \circ f)[x]$.
2. **Case 2:** $x \in B \Leftrightarrow x \notin A$
   - If $x \in B$, then $f[x] = x$ (since f leaves elements outside its cycle fixed). Therefore,

     $$(f \circ g)[x] = f[g[x]] = f[g[x]]$$

     and

     $$(g \circ f)[x] = g[f[x]] = g[x]$$

     Thus, $(f \circ g)[x] = (g \circ f)[x]$.
3. **Case 3:** $x \notin A$ and $x \notin B$
   - If x is not in either cycle, then both f and g leave x fixed. Therefore,

     $$(f \circ g)[x] = f[g[x]] = f[x] = x$$

     and

     $$(g \circ f)[x] = g[f[x]] = g[x] = x$$

     Thus, $(f \circ g)[x] = (g \circ f)[x]$.

Theorem 2.3.5: Disjoint cycle decomposition (p51)

Let $n \in \mathbb{N}$ and let A be a **finite (!)** set with cardinality $|A| = n$. Then every permutation $f \in S_A$ can be written as a composition of **mutually disjoint** cycles:

$$f = c_1 \circ c_2 \circ \dots \circ c_l$$

Note that the **identity permutation** $\text{id} \in S_A$ is a composition of n mutually disjoint 1-cycles:

$$\text{id} = (1)(2)(3)\cdots(n)$$

Corollary 2.3.6: Uniqueness of DCD up to ordering (p52)

Let $n \in \mathbb{N}$ and let A be a set with cardinality $|A| = n$. Further let $f \neq \text{id} \in S_A$ be a permutation *distinct from the identity* permutation. Suppose

$$f \quad = \quad c_1 \circ c_2 \circ \cdots \circ c_l \quad = \quad d_1 \circ d_2 \circ \cdots \circ d_k$$

are two decompositions of f into mutually disjoint cycles. Then

- $l = k$
- After reordering if necessary, $c_i = d_i$ for all $i = 1, 2, \ldots, l$.

If the **1-cycles are removed**, there is *essentially* only **one way** to write f as a composition of mutually disjoint cycles.

The "essentially" in this statement just means that the only freedom one has is to **change ordering** of the cycles in the composition, which does not really matter since **disjoint cycles commute**.

Definition 2.3.9: Type of a permutation (p53)

Let A be a set with cardinality $|A| = n$ and let $f \in S_A$ be a permutation. Suppose that the disjoint cycle decomposition of f has the form $f = c_1 \circ c_2 \circ \cdots \circ c_l$, where

- f has t_1 fixed points (1-cycles),
- f has t_i i-cycles for $i = 2, 3, \ldots, n$

Then the **cycle type** of f is defined as the n-tuple

$$(t_1, t_2, \ldots, t_n)$$

If $f \in S_A$ has cycle type $(t_1, t_2, \ldots, t_n)$, then - since there are only n elements in A - it must hold that

$$t_1 + 2t_2 + 3t_3 + \cdots + nt_n = n$$

Proposition 2.3.12: Order of a permutation based on DCD (p54)

Let A be a **finite** set with cardinality $|A| = n$ and let $f \in S_A$ have a disjoint cycle decomposition $f = c_1 \circ c_2 \circ \cdots \circ c_l$, where c_i is an m_i-cycle for $i = 1, 2, \ldots, l$. Then

$$\operatorname{ord}(f) = \operatorname{lcm}(m_1, m_2, \ldots, m_l)$$

So to determine the order of a permutation, it is sufficient to know its cycle type.