Chapter 1

Sets and Functions

(집합과 함수)

Linear Algebra pp. 1-17

HWP: [Ctrl]+[K], [P]
Adobe Reader: [Ctrl]+[L]

Contents

Notation and Terminology

Functions

- A **function** $f : S \to T$ is a pairing of elements from S and T such that each element $s \in S$ is associated with exactly one element $t \in T$, which is then denoted $f(s)$.
- If $f(s) = t$, we also say that t is the **image** of s under f.
- The set S is called the **domain** of f, the set T is called its **codomain**.
- The **range** of f is $\operatorname{ran}(f) = \operatorname{Im}(f) = \{t \in T \mid \exists\, s \in S : t = f(s)\}$.

One–To–One Functions

- The function f is called injective or one–to–one if it satisfies
$$f(s) = f(s') \implies s = s'$$
for all s and s' in S. One may say that f separates points.
- The function f is called surjective or onto if $\mathrm{Im}(f) = T$.
- The function f is called bijective or one–to–one correspond if it is both injective and surjective.

Composition of Functions

If $f : S \to T$ and $g : T \to U$ are functions, then the **composition** $g \circ f : S \to U$ the function defined by $(g \circ f)(s) = g(f(s))$ for all $s \in S$.

Composition is often represented by a **commutative diagram**:

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[dr, "g \circ f"'] & T \arrow[d, "g"] \\ & U \end{tikzcd}$$

This indicates that an element taking either path from S to U arrives at the same image. Note that for any function $f : S \to T$ we have

$$f \circ 1_S = f \text{ and } 1_T \circ f = f.$$

Composition of Functions

pp.4–5

Proposition 1.1

Let there be given functions $f : S \to T$, $g : T \to U$, $h : U \to V$. Then

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

Thus composition of functions, when defined, is associative.

Proposition 1.2

Let there be given functions $f : S \to T$ and $g : T \to U$. Then

(i) if both f and g are injective, then so is $g \circ f$;

(ii) if both f and g are surjective, then so is $g \circ f$;

(iii) if both f and g are bijective, then so is $g \circ f$;

(iv) if $g \circ f$ is injective, then so is f;

(v) if $g \circ f$ is surjective, then so is g.

(The proofs are left as exercises.)

Inverse Functions

Let $f : S \to T$ be a function. Then f is called invertible if there exists a function $g : T \to S$ such that

$$g \circ f = 1_S \text{ and } f \circ g = 1_T.$$

In this case g is called the **inverse function** of f.

Note the symmetry of the definition, i.e., if g is an inverse function of f, then f is an inverse function of g.

Inverse Functions

Proposition 1.3

If f is invertible, then its inverse is unique.

Theorem 1.4

A function $f : S \to T$ is invertible if and only if it is bijective.

(The proofs are left as exercises.)

Cardinality of a Set

- Let S and T be nonempty sets. Then one says that S and T are of the **same cardinality** if there exists a bijection $f: S \to T$. In this case we writes $\text{Card}(S) = \text{Card}(T)$ or $S \approx T$.
- If S and the set $\{1, 2, 3, \cdots, n\}$ are of the same cardinality for some natural number n, then we say S is a **finite set** and write $\text{Card}(S) = n$.
- If there exists an injective function $f: S \to T$, then we write $\text{Card}(S) \leq \text{Card}(T)$.
- If $\text{Card}(S) \leq \text{Card}(T)$ but there is no bijection $f: S \to T$, then we write $\text{Card}(S) < \text{Card}(T)$.

Theorem. (Schröder–Bernstein)

If $\mathrm{Card}(S) \leq \mathrm{Card}(T)$ and $\mathrm{Card}(T) \leq \mathrm{Card}(S)$, then $\mathrm{Card}(S) = \mathrm{Card}(T)$.

Examples.

(1) $\mathrm{Card}(\mathbb{N}) = \mathrm{Card}(\mathbb{Z})$

(2) $\mathrm{Card}(\mathbb{Z}) = \mathrm{Card}(\mathbb{Q})$

(3) $\mathrm{Card}(\mathbb{Q}) < \mathrm{Card}(\mathbb{R})$

(4) $\mathrm{Card}(\mathbb{R}) = \mathrm{Card}(\mathbb{C})$

(5) $\mathrm{Card}(S) < \mathrm{Card}(\wp(S))$ (Cantor's theorem)

Continuum Hypothesis

Does there exists a set X such that $\mathrm{Card}(\mathbb{N}) < \mathrm{Card}(X) < \mathrm{Card}(\mathbb{R})$?

Symmetric Group

Let $P_n = \{1,\ 2,\ 3,\ \cdots,\ n\}$ denote the set consisting of the first n positive integers.

The set

$$S_n = \{f \mid f \text{ is a bijective function from } P_n \text{ to } P_n\}$$

with composition operation is called the **symmetric group** on n letters.

Elements of S_n are called **permutations**.

Example. Let $n = 3$. We list the permutations by 2×3 arrays each of which shows the image of each number directly below it.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Composition Operations in Symmetric Groups

(i) Composition is an associative operation on S_n. In particular, S_n is closed under composition of functions.

(ii) The identity map in S_n acts as an identity element with respect to composition.

(iii) For every element f in S_n, there is an element g in S_n such that

$$f \circ g = g \circ f = 1_{P_n},$$

that is, every element of S_n has an inverse in S_n.

Proposition 1.5

The cardinality of S_n is $n!$.

Transposition

Let $a_1,\ a_2,\ \cdots,\ a_k$ be k distinct numbers in $\{1,\ 2,\ 3,\ \cdots,\ n\}$. Then the **$k$-cycle**

$$(a_1\ a_2\ a_3\ \cdots\ a_k)$$

is the permutation defined by the following assignments:

$$a_1 \mapsto a_2,\quad a_2 \mapsto a_3,\quad \cdots,\quad a_{k-1} \mapsto a_k,\quad a_k \mapsto a_1.$$

All other numbers are unaffected. In the special case of a 2-cycle, we speak of a **transposition**.

We shall see shortly that all permutations may be constructed from transpositions.

Examples

(1) In S_5, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} = (1\ 4\ 5\ 2)$.

(2) In S_5, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3\ 4) \circ (2\ 5)$.

(3) In S_6, $\pi = (4\ 5) \circ (1\ 3\ 6\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix}$.

In fact, every permutation is expressible as the product of disjoint cycles.

Moreover, every cycle can be written as the product of transpositions. For example,

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

Thus every permutation can be factored into a product of transpositions.

Theorem. (Invariance of Parity)
Suppose that a permutation may be expressed as the product of an even number of transpositions. Then every factorization into transpositions likewise involves an even number of factors. Similarly, if a permutation may be expressed as the product of an odd number of transpositions, then every such factorization involves an odd number of transpositions.

The proof of this theorem depends upon the construction of a map

$$\sigma : S_n \to \{-1, 1\}$$

called the sign homomorphism. Its definition follows(next page).

Let π lie in S_n. We say that π reverses the pair (i, j), if $i < j$, but $\pi(j) < \pi(i)$.

It is easy to count the number of reversals when a permutation is expressed in matri form: for every element in the second row, we count how many smaller elements lie to the right. For example, the permutation

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

has $3+1+3+0+0+0=7$ reversals. Now if π has m reversals, define

$$\sigma(\pi) = (-1)^m.$$

Hence the sign map is negative for permutations that have an odd number of reversals and positive for those that have an even number of reversals. It is clear that a transposition of adjacent elements, having exactly one reversal, has sign -1.

The key result is this:

Lemma 1.7 Let π be a permutation and τ a transposition. Then

$$\sigma(\tau \circ \pi) = -\sigma(\pi).$$

Thus composition with a transposition changes the sign of a permutation.

Proof. Assume that $\pi \in S_n$ has the representation

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ a_1 & a_2 & \cdots & a_i & \cdots & a_j & \cdots & a_n \end{pmatrix}.$$

We ask what effect the transposition $(a_i\ a_j)$ has on π. To swap a_i and a_j we must first push a_i to the right across $j-i$ entries. (This amounts to $j-i$ adjacent transpositions.)

(continue)

(continued)

Each move either adds or subtracts a reversal and hence changes the sign of the permutation once. We must next push a_j to the left across $j-i-1$ entries (one fewer), again changes. Since this number is manifestly odd, the sign of $\tau \circ \pi$ has indeed been changed relative to π, as claimed. □

By repeated use of the lemma it follows that for the product of m transpositions

$$\sigma(\tau_1 \circ \tau_2 \circ \cdots \circ \tau_m) = (-1)^m.$$

Suppose we have two equal products of transpositions

$$\tau_1 \circ \tau_2 \circ \cdots \circ \tau_m = \omega_1 \circ \omega_2 \circ \cdots \circ \omega_{m'}.$$

Then applying σ to both sides, we find that $(-1)^m = (-1)^{m'}$ and therefore m and m' have the same parity, as claimed. □

We Learned

- ✓ Notation and Terminology
- ✓ Composition of Functions
- ✓ Inverse Functions
- ✓ Cardinality
- ✓ Permutations

Homework

- Search Google to find the proof for Schröder–Bernstein theorem.
- Find the cardinality of the set consisting of all the functions from $\mathbb{N}$ to $\mathbb{N}$.
- Construct an algorithm to express a permutation as a product of transpositions.