Preliminaries

Some results and notation that are used throughout the text are collected in this chapter for convenience. Students may wish to review this chapter quickly at first and then read each section more carefully again as the concepts appear in the course of the text.

0.1 BASICS

The basics of set theory: sets, $\cap, \cup, \in$, etc. should be familiar to the reader. Our notation for subsets of a given set A will be

$$B = \{a \in A \mid \ldots \text{ (conditions on a) } \ldots\}.$$

The *order* or *cardinality* of a set A will be denoted by $|A|$. If A is a finite set the order of A is simply the number of elements of A.

It is important to understand how to test whether a particular $x \in A$ lies in a subset B of A (cf. Exercises 1-4). The *Cartesian product* of two sets A and B is the collection $A \times B = \{(a, b) \mid a \in A, b \in B\}$, of ordered pairs of elements from A and B.

We shall use the following notation for some common sets of numbers:

(1) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ denotes the *integers* (the $\mathbb{Z}$ is for the German word for numbers: "Zahlen").

(2) $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ denotes the *rational numbers* (or *rationals*).

(3) $\mathbb{R} = \{$ all decimal expansions $\pm d_1 d_2 \ldots d_n . a_1 a_2 a_3 \ldots \}$ denotes the *real numbers* (or *reals*).

(4) $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$ denotes the *complex numbers*.

(5) $\mathbb{Z}^+, \mathbb{Q}^+$ and $\mathbb{R}^+$ will denote the positive (nonzero) elements in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively.

We shall use the notation $f : A \to B$ or $A \xrightarrow{f} B$ to denote a function f from A to B and the value of f at a is denoted $f(a)$ (i.e., we shall apply all our functions on the left). We use the words *function* and *map* interchangeably. The set A is called the *domain* of f and B is called the *codomain* of f. The notation $f : a \mapsto b$ or $a \mapsto b$ if f is understood indicates that $f(a) = b$, i.e., the function is being specified on *elements*.

If the function f is not specified on elements it is important in general to check that f is *well defined*, i.e., is unambiguously determined. For example, if the set A is the union of two subsets A_1 and A_2 then one can try to specify a function from A

to the set $\{0, 1\}$ by declaring that f is to map everything in A_1 to 0 and is to map everything in A_2 to 1. This unambiguously defines f unless A_1 and A_2 have elements in common (in which case it is not clear whether these elements should map to 0 or to 1). Checking that this f is well defined therefore amounts to checking that A_1 and A_2 have no intersection.

The set

$$f(A) = \{b \in B \mid b = f(a), \text{ for some } a \in A\}$$

is a subset of B, called the *range* or *image* of f (or the *image of* A *under* f). For each subset C of B the set

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

consisting of the elements of A mapping into C under f is called the *preimage* or *inverse image* of C under f. For each $b \in B$, the preimage of $\{b\}$ under f is called the *fiber* of f over b. Note that f^{-1} is not in general a function and that the fibers of f generally contain many elements since there may be many elements of A mapping to the element b.

If $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by

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

Let $f : A \to B$.

(1) f is *injective* or is an *injection* if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

(2) f is *surjective* or is a *surjection* if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$, i.e., the image of f is *all* of B. Note that since a function always maps onto its range (by definition) it is necessary to specify the codomain B in order for the question of surjectivity to be meaningful.

(3) f is *bijective* or is a *bijection* if it is both injective and surjective. If such a bijection f exists from A to B, we say A and B are in *bijective correspondence*.

(4) f has a *left inverse* if there is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A, i.e., $(g \circ f)(a) = a$, for all $a \in A$.

(5) f has a *right inverse* if there is a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.

Proposition 1. Let $f : A \to B$.

(1) The map f is injective if and only if f has a left inverse.

(2) The map f is surjective if and only if f has a right inverse.

(3) The map f is a bijection if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A.

(4) If A and B are finite sets with the same number of elements (i.e., $|A| = |B|$), then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.

Proof: Exercise.

In the situation of part (3) of the proposition above the map g is necessarily unique and we shall say g is the *2-sided inverse* (or simply the *inverse*) of f.

A *permutation* of a set A is simply a bijection from A to itself.

If $A \subseteq B$ and $f : B \to C$, we denote the *restriction* of f to A by $f|_A$. When the domain we are considering is understood we shall occasionally denote $f|_A$ again simply as f even though these are formally different functions (their domains are different).

If $A \subseteq B$ and $g : A \to C$ and there is a function $f : B \to C$ such that $f|_A = g$, we shall say f is an *extension* of g to B (such a map f need not exist nor be unique).

Let A be a nonempty set.

(1) A *binary relation* on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.

(2) The relation $\sim$ on A is said to be:

(a) *reflexive* if $a \sim a$, for all $a \in A$,

(b) *symmetric* if $a \sim b$ implies $b \sim a$ for all $a, b \in A$,

(c) *transitive* if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.

A relation is an *equivalence relation* if it is reflexive, symmetric and transitive.

(3) If $\sim$ defines an equivalence relation on A, then the *equivalence class* of $a \in A$ is defined to be $\{x \in A \mid x \sim a\}$. Elements of the equivalence class of a are said to be *equivalent* to a. If C is an equivalence class, any element of C is called a *representative* of the class C.

(4) A *partition* of A is any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A (I some indexing set) such that

(a) $A = \cup_{i \in I} A_i$, and

(b) $A_i \cap A_j = \emptyset$, for all $i, j \in I$ with $i \neq j$

i.e., A is the disjoint union of the sets in the partition.

The notions of an equivalence relation on A and a partition of A are the same:

Proposition 2. Let A be a nonempty set.

(1) If $\sim$ defines an equivalence relation on A then the set of equivalence classes of $\sim$ form a partition of A.

(2) If $\{A_i \mid i \in I\}$ is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets $A_i, i \in I$.

Proof: Omitted.

Finally, we shall assume the reader is familiar with proofs by induction.

EXERCISES

In Exercises 1 to 4 let $\mathcal{A}$ be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix} .$$

Let

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

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

1. Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$ (where $+$ denotes the usual sum of two matrices).

3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ (where $\cdot$ denotes the usual product of two matrices).

4. Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

5. Determine whether the following functions f are well defined:
(a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.
(b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

7. Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

0.2 PROPERTIES OF THE INTEGERS

The following properties of the integers $\mathbb{Z}$ (many familiar from elementary arithmetic) will be proved in a more general context in the ring theory of Chapter 8, but it will be necessary to use them in Part I (of course, none of the ring theory proofs of these properties will rely on the group theory).

(1) (Well Ordering of $\mathbb{Z}$) If A is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$ (m is called a *minimal element* of A).

(2) If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. In this case we write $a \mid b$; if a does not divide b we write $a \nmid b$.

(3) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer d, called the *greatest common divisor of a and b* (or g.c.d. of a and b), satisfying:
(a) $d \mid a$ and $d \mid b$ (so d is a common divisor of a and b), and
(b) if $e \mid a$ and $e \mid b$, then $e \mid d$ (so d is the greatest such divisor).
The g.c.d. of a and b will be denoted by (a, b). If $(a, b) = 1$, we say that a and b are *relatively prime*.

(4) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer l, called the *least common multiple of a and b* (or l.c.m. of a and b), satisfying:
(a) $a \mid l$ and $b \mid l$ (so l is a common multiple of a and b), and
(b) if $a \mid m$ and $b \mid m$, then $l \mid m$ (so l is the least such multiple).
The connection between the greatest common divisor d and the least common multiple l of two integers a and b is given by $dl = ab$.

(5) The *Division Algorithm*: if $a, b \in \mathbb{Z} - \{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|,$$