CRYPTOGRAPHY TOPIC II
SETS AND FUNCTIONS

PAUL L. BAILEY

Abstract. This document includes the basic definitions regarding sets and functions which are universal in mathematics.

1. Sets and Elements

A *set* is a collection of *elements*. The elements of a set are sometimes called *members* or *points*. We assume that we can distinguish between different elements, and that we can determine whether or not a given element is in a given set.

The relationship of two elements a and b being the same is *equality* and is denoted $a = b$. The negation of this relation is denoted $a \neq b$, that is, $a \neq b$ means that it is not the case that $a = b$.

The relationship of an element a being a member of a set A is *containment* and is denoted $a \in A$. The negation of this relation is denoted $b \notin A$, that is, $b \notin A$ means that it is not the case that $b \in A$.

A set is determined by the elements it contains. That is, two sets are considered equal if and only if they contain the same elements. We use the symbols "$\Rightarrow$" to mean "implies", and "$\Leftrightarrow$" to mean "if and only if". Then

$$A = B \quad \Leftrightarrow \quad (a \in A \Leftrightarrow a \in B).$$

Thus we should not think of a set as a "container", but rather as the things being contained. For example, consider a glass of water, and the set of water molecules in the glass. If we pour all of the water into an empty bowl, the bowl now contains the same set of water molecules.

One way of describing a set is by explicitly listing its members. Such lists are surrounded by braces, e.g., the set of the first five prime integers is $\{2, 3, 5, 7, 11\}$. If the pattern is clear, we may use dots; for example, to label the set of all prime numbers as P, we may write $P = \{2, 3, 5, 7, 11, 13, \dots\}$. Thus $2 \in P$ and $23 \in P$, but $1 \notin P$ and $21 \notin P$. As another example, if we denote the set of all integers by $\mathbb{Z}$, we may write $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. Note that the order of elements in a list is irrelevant in determining a set, for example, $\{5, 3, 7, 11, 2\} = \{2, 3, 5, 7, 11\}$. Also, there is no such thing as the "multiplicity" of an element in a set, for example $\{1, 3, 2, 2, 1\} = \{1, 2, 3\}$.

2. Subsets

If A and B are sets and all of the elements in A are also contained in B, we say that A is a *subset* of B or that A is *included* in B and write $A \subset B$:

$$A \subset B \quad \Leftrightarrow \quad (a \in A \Rightarrow a \in B).$$

Date: September 6, 2007.

For example, $\{1,3,5\} \subset \{1,2,3,4,5\}$. Note that any set is a subset of itself. We say that A is a *proper subset* of B is $A \subset B$ but $A \neq B$.

It follows immediately from the definition of subset that

$$A = B \quad \Leftrightarrow \quad (A \subset B \text{ and } B \subset A).$$

Thus to show that two sets are equal, it suffices to show that each is contained in the other.

A set containing no elements is called the *empty set* and is denoted $\varnothing$. Since a set is determined by its elements, there is only one empty set. Note that the empty set is a subset of any set.

3. Set Operations

We may construct new sets as subsets of existing sets by specifying properties. Specifically, we may have a proposition $p(x)$ which is true for some elements x in a set X and not true for others. Then we may construct the set

$$\{x \in X \mid p(x) \text{ is true}\};$$

this is read "the set of x in X such that $p(x)$". The construction of this set is called *specification.* For example, if we let $\mathbb{Z}$ be the set of integers, the set P of all prime numbers could be specified as $P = \{n \in \mathbb{Z} \mid n \text{ is prime}\}$.

Let A and B be subsets of some "universal set" U and define the following set operations:

$$\begin{aligned} \text{Union:} \qquad & A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\} \\ \text{Intersection:} \qquad & A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\} \\ \text{Complement:} \qquad & A \setminus B = \{x \in U \mid x \in A \text{ and } x \notin B\} \end{aligned}$$

The pictures which correspond to these operations are called *Venn diagrams.*

Example 1. Let $A = \{1,3,5,7,9\}$, $B = \{1,2,3,4,5\}$. Then $A \cap B = \{1,3,5\}$, $A \cup B = \{1,2,3,4,5,7,9\}$, $A \setminus B = \{7,9\}$, and $B \setminus A = \{2,4\}$. □

Example 2. Let A and B be two distinct nonparallel lines in a plane. We may consider A and B as sets of points. Their intersection is a set containing a single point, their union is a set consisting of all points on crossing lines, and the complement of A with respect to B is A minus the point of intersection. □

If $A \cap B = \varnothing$, we say that A and B are *disjoint.*

Example 3. A *sphere* is the set of points in space equidistant from a given point, called its *center*; the common distance to the center is called that *radius* of the sphere. Thus a sphere is the surface of a solid ball.

Take two points in space such that the distance between them is 10, and imagine two spheres centered at these points. Let one of the spheres have radius 5. If the radius of the other sphere is less than 5 or greater than 15, then the spheres are disjoint. If the radius of the other sphere is exactly 5 or 15, the intersection is a single point. If the radius of the other sphere is between 5 and 15, the spheres intersect in a circle. □

The following properties are sometimes useful.

- $A = A \cup A = A \cap A$
- $\varnothing \cap A = \varnothing$
- $\varnothing \cup A = A$
- $A \subset B \Leftrightarrow A \cap B = A$
- $A \subset B \Leftrightarrow A \cup B = B$

The following properties state that union and intersection are commutative and associative operations, and that they distribute over each other. These properties are intuitively clear via Venn diagrams.

- $A \cap B = B \cap A$
- $A \cup B = B \cup A$
- $(A \cap B) \cap C = A \cap (B \cap C)$
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
- $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Since $(A \cap B) \cap C = A \cap (B \cap C)$, parentheses are useless and we write $A \cap B \cap C$. This extends to four sets, five sets, and so on. Similar remarks apply to unions.

The following properties of complement are known as *DeMorgan's Laws.* You should draw Venn diagrams of these situations to convince yourself that these properties are true.

- $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$
- $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$

Here are a few more properties of complement:

- $A \subset B \Rightarrow A \cup (B \smallsetminus A) = B$;
- $A \subset B \Rightarrow A \cap (B \smallsetminus A) = \varnothing$;
- $A \smallsetminus (B \smallsetminus C) = (A \smallsetminus B) \cup (A \cap B \cap C)$;
- $(A \smallsetminus B) \smallsetminus C = A \smallsetminus (B \cup C)$.

4. Cartesian Product

Let a and b be elements. The *ordered pair* of a and b is denoted (a, b) and is defined as

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

This is the technical definition; think about how it relates to the intuitive approach below.

Intuitively, if a and b are elements, the *ordered pair* with first coordinate a and second coordinate b is something like a set containing a and b, but in such a way that the order matters. We denote this ordered pair by (a, b) and declare that it has the following "defining property":

$$(a, b) = (c, d) \quad \Leftrightarrow \quad (a = c \text{ and } b = d).$$

The *cartesian product* of the sets A and B is denoted $A \times B$ and is defined to be the set of all ordered pairs whose first coordinate is in A and whose second coordinate is in B:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Example 4. Let $A = \{1, 3, 5\}$ and let $B = \{1, 4\}$. Then

$$A \times B = \{(1, 1), (1, 4), (3, 1), (3, 4), (5, 1), (5, 4)\}.$$

In particular, this set contains 6 elements. □

In general, if A contains m elements and B contains n elements, where m and n are natural numbers, then $A \times B$ contains mn elements. Consider the case where $A = B$; then $A \times A$ contains m^2 elements. We sometimes write A^2 to mean $A \times A$.

We have the following properties:

- $(A \cup B) \times C = (A \times C) \cup (B \times C)$;
- $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
- $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

5. Numbers

The following familiar sets of numbers have standard names:

Natural Numbers:	$\mathbb{N} = \{0, 1, 2, 3, \dots\}$
Integers:	$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
Rational Numbers:	$\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$
Real Numbers:	$\mathbb{R} = \{$ numbers given by decimal expansions $\}$
Complex Numbers:	$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}$ and $i^2 = -1\}$

We have $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

The following standard notation gives subsets of the real numbers, called *intervals*:

- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ (closed)
- $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ (open)
- $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$
- $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$
- $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$ (closed)
- $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$ (open)
- $[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$ (closed)
- $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$ (open)

Example 5. Let $A = [1, 5]$ be the closed interval of real numbers between 1 and 5 and let $B = (10, 16)$ be the open interval of real numbers between 10 and 16. Let $C = A \cup B$. Let $\mathbb{N}$ be the set of natural numbers. How many elements are in $C \cap \mathbb{N}$?

Solution. We know that

$$C \cap \mathbb{N} = (A \cup B) \cap \mathbb{N} = (A \cap \mathbb{N}) \cup (B \cap \mathbb{N}).$$

Now $A \cap \mathbb{N}$ is the set of natural numbers between 1 and 5, inclusive, so $A \cap \mathbb{N} = \{1, 2, 3, 4, 5\}$. Also, $B \cap \mathbb{N}$ is the set of natural number between 10 and 16, exclusive, so $B \cap \mathbb{N} = \{11, 12, 13, 14, 15\}$. Now $C \cap \mathbb{N}$ is the union of these set, so $C \cap \mathbb{N} = \{1, 2, 3, 4, 5, 11, 12, 13, 14, 15\}$. Therefore $C \cap \mathbb{N}$ has 10 elements. □

Example 6. Let $A = [1, 4]$ and $B = [3, 8)$ be intervals of real numbers. We will see how to view $A \times B$ as a square in the cartesian plane $\mathbb{R}^2$ which has a boundary on three sides but not of the fourth. How many elements are in $(A \times B) \cap (\mathbb{Z} \times \mathbb{Z})$?

Solution. By a previously stated property of cartesian product, we have

$$(A \times B) \cap (\mathbb{Z} \times \mathbb{Z}) = (A \cap \mathbb{Z}) \times (B \cap \mathbb{Z}).$$

Now $A \times \mathbb{Z} = \{1, 2, 3, 4\}$ and $B \times \mathbb{Z} = \{3, 4, 5, 6, 7\}$. Thus $(A \times B) \cap (\mathbb{Z} \times \mathbb{Z})$ has $4 \cdot 5 = 20$ elements. □

Warning 1. The notation for ordered pair (a, b) is the same as the standard notation for open interval of real numbers, but its meaning is entirely different. This is standard, and you must decide from the context which meaning is intended.

6. Functions

Let A and B be sets. A *function* from A to B is a subset $f \subset A \times B$ of the cartesian product of A with B such that for every $a \in A$ there exists a unique $b \in B$ with $(a, b) \in f$. This is the technical definition; think about how it relates to the intuitive approach below.

Intuitively, a *function* from a set A to a set B is an assignment of every element in A to some element in B. Another way of describing this is that we think of a function as a kind of vehicle, something which sends each element of A to an element of B. If we think of elements as the nouns of set theory and sets as the adjectives (an element has a property if it is in the set of things with that property), then we may think of functions as the verbs.

We will study many familiar examples of functions from the set of real numbers into itself, for example, polynomial functions, rational functions, trigonometric functions, exponent functions, and logarithmic functions. We will also see functions from A to B where A and B are not necessarily sets of real numbers. It is essential in mathematics, and useful as a way of thinking in general, to expand our view of functions so that they can send elements from any set to any other set.

Let f be a function from A to B. If $a \in A$, the element of B to which a is assigned by f is denoted $f(a)$; in other words, the place in B to which a is sent by f is denoted $f(a)$. We declare that a function must satisfy the following "defining property":

$$\text{for every } a \in A \text{ there exists a unique } b \in B \text{ such that } f(a) = b.$$

If f is a function from A to B, this fact is denoted

$$f : A \to B.$$

We say that f *maps* A *into* B, and that f is a function *on* A. For this reason, functions are sometimes called *maps* or *mappings*. If $f(a) = b$, we say that a is *mapped to* b by f. We may indicate this by writing $a \mapsto b$.

Two functions $f : A \to B$ and $g : A \to B$ are considered *equal* if they act the same way on every element of A:

$$f = g \quad \Leftrightarrow \quad (a \in A \Rightarrow f(a) = g(a)).$$

Thus to show that two functions f and g are equal, select an arbitrary element $a \in A$ and show that $f(a) = g(a)$.

If A is sufficiently small, we may explicitly describe the function by listing the elements of A and where they go; for example, if $A = \{1, 2, 3\}$ and $B = \mathbb{R}$, a perfectly good function is described by $\{1 \mapsto 23.432, 2 \mapsto \pi, 3 \mapsto \sqrt{593}\}$.

However, if A is large, the functions which are easiest to understand are those which are specified by some *rule* or *algorithm.* The common functions of single variable calculus are of this nature.

Example 7. The following can be functions from $\mathbb{R}$ into $\mathbb{R}$:

- $f(x) = 0$;
- $f(x) = x$;
- $f(x) = x^3 + 3x + 17$.

The following can be functions from the set of positive real numbers into $\mathbb{R}$:

- $f(x) = \frac{1}{x}$;
- $f(x) = \sqrt{x}$.

Note that $\frac{1}{x}$ is not a function from $\mathbb{R}$ into $\mathbb{R}$, because it is not defined at $x = 0$. □

Some functions are constructed from existing functions by specifying cases.

Example 8. Let $\mathbb{R}$ be the set of real numbers. Define $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} x^2 + 2 & \text{if } x < 0; \\ x^3 - 1 & \text{if } x \geq 0. \end{cases}$$

Then, for example, $f(-2) = (-2)^2 + 2 = 6$ and $f(2) = 2^3 - 1 = 7$. □

Example 9. Let X be a set and let $A \subset X$. The *characteristic function* of A in X is a function $\chi_A : X \to \{0, 1\}$ defined by

$$\chi_A(x) = \begin{cases} 0 \text{ if } x \notin A; \\ 1 \text{ if } x \in A. \end{cases}$$

In particular, let $X = [0, 1] \subset \mathbb{R}$ be the closed unit interval and let $A = \mathbb{Q} \cap X$ be the set of rational numbers in this interval. Think about the graph of the function χ_A. □

Example 10. Suppose we designed a computer system that records information on patients in a hospital. Each patient is assigned a number upon admission, which is just the next available number, starting with zero. We create a program which allows the user to type a working diagnosis of up to 60 characters or less for this patient, and file this information under the patient number. We only allow the user to type capital letters, spaces, commas, and periods in this diagnosis. Trailing spaces in the diagnosis are automatically removed. The file may be viewed as a function

$$\text{DIAG(patient number)} = \text{“patient diagnosis”};$$

here, DIAG : $\mathbb{N} \to B$, where B is the set of all possible strings of allowed characters with length less than or equal to 60 and no trailing spaces. The size of B is 29^{60} (why?). □

7. Images and Preimages

If $f : A \to B$, the set A is called the *domain* of the function and the set B is called the *codomain.* We often think of a function as taking the domain A and placing it in the codomain B. However, when it does so, we must realize that more than one element of A can be sent to a given element in B, and that there may be some elements in B to which no elements of A are sent.

If $a \in A$, the *image* of a under f is $f(a)$.

If $b \in B$, the *preimage* of b is a subset of A given by

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

If $C \subset A$, we define the *image* of C under f to be the set

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

The image of the domain is called the *range* of the function.

If $D \subset B$, we define the *preimage* of D under f to be the set

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

Notice that $f^{-1}(b)$ is not necessarily a singleton subset of A. For example, if $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$, then the preimage of the point 4 is

$$f^{-1}(4) = \{2, -2\}.$$

A function $f : A \to B$ is called *surjective* (or *onto*) if

$$\text{for every } b \in B \text{ there exists } a \in A \text{ such that } f(a) = b.$$

Equivalently, f is surjective if $f(A) = B$. This says that every element in B is "hit" by some element from A.

A function $f : A \to B$ is called *injective* (or *one-to-one*) if

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Equivalently, f is injective if for all $b \in B$, $f^{-1}(b)$ contains at most one element in A.

A function $f : A \to B$ is called *bijective* if it is both injective and surjective. Such a function sets up a *correspondence* between the elements of A and the elements of B.

Example 11. First we consider "real-valued functions of a real variable". This simply means that the domain and the codomain of the function are subsets of $\mathbb{R}$.

- $f(x) = x^3$ is bijective;
- $g(x) = x^2$ is neither injective nor surjective;
- $h(x) = x^3 - 2x^2 - x + 2$ is surjective but not injective;
- $e(x) = 2^x$ is injective but not surjective.

Let $A = \{-1, 1, 2\}$. Some of the images and preimages of A are:

- $f(A) = \{-1, 1, 8\}$;
- $g(A) = \{1, 4\}$;
- $h(A) = \{0\}$;
- $f^{-1}(A) = \{-1, 0, \sqrt[3]{2}\}$;
- $g^{-1}(A) = \{-\sqrt[3]{2}, -1, 1, \sqrt[3]{2}\}$;
- $a^{-1}(A) = \varnothing$.

Example 12. Let $\mathbb{N}$ be the set of natural numbers and let $\mathbb{Z}$ be the set of integers. The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $n \mapsto 2n$ is injective but not surjective.

The function $g : \mathbb{Z} \to \mathbb{N}$ given by $n \mapsto \sqrt{n^2}$ is surjective but not injective. The preimage of $5 \in \mathbb{N}$ under g is $\{-5, 5\}$.

The function $h : \mathbb{Z} \to \mathbb{Z}$ given by $n \mapsto -n$ is bijective. □

Example 13. Let A be the set of all animals in a zoo and let B be the set of all species of animals on earth. Then we obtain a function $f : A \to B$ by defining $f(a) = b$, where the species of animal a is b. This function is surjective only if this is an unbelievably excellent (and large) zoo, for this would mean it has at least one animal of every species on earth. It is injective only if every animal is very lonely, for this would mean that the zoo contains at most one animal of a given species.

However, a function which assigns to every animal on Noah's Ark its species would be surjective but not injective, since he had two of every kind. Such a function is sometimes called "two-to-one". □

Example 14. If DIAG is a function which assigns to a patient his diagnosis, then DIAG is injective unless two patients have the same diagnosis. For this function to be surjective, we must have admitted at least 29^{60} patients. □

8. Composition of Functions

Let A, B, and C be sets and let $f : A \to B$ and $g : B \to C$. The *composition* of f and g is the function

$$g \circ f : A \to C$$

given by

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

The domain of $g \circ f$ is A and the codomain is C. The range of $g \circ f$ is the image under g of the image under f of the domain of f.

Example 15. Let A be the set of living things on earth, B the set of species, and C be the set of positive real numbers. Let $f : A \to B$ assign each living thing to its species, and let $g : B \to C$ assign each species to its average mass. Then $g \circ f$ guesses the mass of a living thing. □

Proposition 1. *Let $f : A \to B$ and $g : B \to C$ be surjective functions. Then $g \circ f : A \to C$ is an surjective function.*

Proposition 2. *Let $f : A \to B$ and $g : B \to C$ be injective functions. Then $g \circ f : A \to C$ is an injective function.*

Example 16. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$ and let $g : \mathbb{R} \to \mathbb{R}$ be given by $g(x) = x - 9$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is given by $g \circ f(x) = x^2 - 9$ and $f \circ g : \mathbb{R} \to \mathbb{R}$ is given by $f \circ g(x) = x^2 - 6x + 9$. □

This example demonstrates that composition of functions is not a commutative operation. However, the next proposition tells us that composition of functions is associative.

Proposition 3. *Let A, B, C, and D be sets and let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

9. Restrictions, Identities, and Inverses

Let $f : X \to Y$ be a function and let $Z = f(X)$ be the range of f. The same function f can be viewed as a function $f : X \to Z$. It is standard in this case to call the function, viewed in this way, by the same name. Note that the function $f : X \to Z$ is surjective. Thus any function is a surjective function onto its range.

Let $f : X \to Y$ be a function and let $A \subset X$ be a subset of the domain of f. The *restriction* of f to A is a function

$$f \upharpoonright_A : A \to Y \text{ given by } f \upharpoonright_A (a) = f(a).$$

Thus given any function and any subset of the domain, there is a function which coincides with the original one, but whose domain is the subset. For example, the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ can certainly be viewed as a function on the integers, sending each integer to its square.

Let A be any set. The *identity function* on A if the function $\mathrm{id}_A : A \to A$ given by $\mathrm{id}_A(a) = a$ for every $a \in A$. Thus the identity function on A is that function which does nothing to A. The identity function has the property that if $g : A \to C$, then $g \circ \mathrm{id}_A = g$, and if $h : D \to A$, then $\mathrm{id}_A \circ h = h$.

Let $f : A \to B$ be a function. We say that f is *invertible* if there exists a function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. In this case we call g the *inverse* of f. The inverse of a function f is often denoted f^{-1}.

If f is not injective, then f cannot be invertible. Sometimes we restrict the domain of f to a subset on which f is injective to invent a partial inverse.

10. Exercises

Exercise 1. Let A, B, and C be the following subsets of $\mathbb{N}$:

- $A = \{n \in \mathbb{N} \mid n \leq 25\}$;
- $E = \{n \in A \mid n \text{ is even}\}$;
- $O = \{n \in A \mid n \text{ is odd}\}$;
- $P = \{n \in A \mid n \text{ is prime}\}$;
- $S = \{n \in A \mid n \text{ is a square}\}$;

Compute the following sets.

(a) $(P \cup S) \cap O$
(b) $(E \smallsetminus S) \cup P$
(c) $(O \cap S) \times (E \cap S)$

Exercise 2. Draw Venn diagrams which demonstrate the following equations.

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(c) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$
(d) $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$

Exercise 3. Let A and B be subsets of a set U. The *symmetric difference* of A and B, denoted $A \triangle B$, is the set of points in U which are in either A or B but not in both.

(a) Draw a Venn diagram describing $A \triangle B$.
(b) Find two set expressions which could be used to define $A \triangle B$. These expressions may use A, B, union, intersection, complement, and parentheses,

Exercise 4. Let P be the set of people who ever lived. Which of the following are functions from P to P?

(a) $\{(a, b) \in P \times P \mid b \text{ is a father of } a\}$
(b) $\{(a, b) \in P \times P \mid a \text{ is a father of } b\}$
(c) $\{(a, b) \in P \times P \mid b \text{ is a grandmother of } a\}$
(d) $\{(a, b) \in P \times P \mid b \text{ is a youngest son of the paternal grandmother of } a\}$
(e) $\{(a, b) \in P \times P \mid b \text{ is a youngest son of the maternal grandmother of } a\}$

Exercise 5. Let $\mathbb{N}$ be the set of natural numbers and let $\mathbb{Z}$ be the integers. Find examples of functions $f : \mathbb{Z} \to \mathbb{N}$ such that:
(a) f is bijective;
(b) f is injective but not surjective;
(c) f is surjective but not injective;
(d) f is neither injective nor surjective.

Exercise 6. Let $\mathbb{N}$ be the set of natural numbers. Let $A = [50, 70] \cap \mathbb{N}$. Define a function $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = 3n$. Note that A is in both the domain and the codomain of f.
(a) Find the image $f(A)$.
(b) Find the preimage $f^{-1}(A)$.
(c) Is f injective? Is f surjective?

Exercise 7. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^3 - 6x^2 + 11x - 3$. Find $f^{-1}(3)$.

Exercise 8. We would like to define a function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ by $(p, q) \mapsto \frac{p}{q}$. Unfortunately, this does not make sense. Fix the problem, so that the resulting function is surjective but not injective.

Exercise 9. We would like to define a function $f : \mathbb{Q} \to \mathbb{Z}$ by $\frac{p}{q} \mapsto pq$. Unfortunately, this is not “well-defined”. Figure out what this means and fix the problem. Is the resulting function injective?

Exercise 10. Let $f : X \to Y$ be a function and let $A, B \subset X$ and $C, D \subset Y$. Which of the following statements are true? If the statement is false, attempt to construct a counterexample.

(a) $f(A \cup B) \subset f(A) \cup f(B)$
(b) $f(A \cup B) = f(A) \cup f(B)$
(c) $f(A \cap B) \subset f(A) \cap f(B)$
(d) $f(A \cap B) = f(A) \cap f(B)$
(e) $f^{-1}(C \cup D) = f^{-1}(C) \cup f(D)$
(f) $f^{-1}(C \cap D) = f^{-1}(C) \cap f(D)$

Exercise 11. Let $f : X \to Y$ be a function. Which of the following statements are true?

(a) f is surjective if and only if there exists $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.
(b) f is injective if and only if there exists $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$.

Exercise 12. Let X be a set containing m elements and let Y be a set containing n elements. How many functions are there from X to Y? How many bijective functions are there from X to Y?

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: `plbailey@saumag.edu`