Math 4030-001/Foundations of Algebra/Fall 2017

Foundations of the Foundations: Sets

A **set** is a collection of objects, which are the **elements** of the set. We denote sets with capital letters, elements with small letters, and

$$a \in A \text{ and } b \notin A$$

means a is an element of the set A and b is **not** an element of A.

There is one set containing no elements, namely the **empty set** $\emptyset$.

A (finite) set is written as the list of its elements:

$$A = \{a, e, d, x, c\}$$

in any order, and no element may appear twice in the list.

Sets A and B have the **same cardinality** if there is a function:

$$f : A \to B$$

that is both one-to-one (injective) and onto (surjective), which is the case exactly when there is an inverse function $f^{-1} : B \to A$.

Remark. A one-to-one and onto (invertible) function is a **bijection**.

Two sets with a finite number of elements have the same cardinality if and only if they have the same number of elements, but there are infinite sets (e.g. natural vs real numbers) with different cardinalities.

The **intersection** $A \cap B$ is the set of elements in both A and B, and the **union** $A \cup B$ is the set of elements in A or B (or both of them). For example, if A is as above and $B = \{b, e, f, y, c\}$, then:

$$A \cap B = \{e, c\} \text{ and } A \cup B = \{a, b, e, d, f, x, y, c\}$$

For sets with finitely many elements, we write:

$$|A| = \text{the number of elements in } A$$

and the "principle of inclusion and exclusion" tells us that:

$$|A| + |B| - |A \cap B| = |A \cup B|$$

Sets A and B are **disjoint** if $A \cap B = \emptyset$.

B is a **subset** of A, written $B \subset A$ if all of the elements of B are elements of A, which is equivalent to each of the following:

$$B = A \cap B \text{ and } A = A \cup B$$

Often we will consider sets that are subsets of one **universe** set U. The sets A and B above are subsets of the universe of (small) letters:

$$U = \{a, b, c, ..., x, y, z\},$$

Within a universe U, the **complement** of A is:

$$A^c = \text{the set of elements in } U \text{ that do } \textbf{not} \text{ belong to } A$$

so, in the example above, A^c is the set of the 21 letters of the alphabet that are not a, e, d, x or c.

A collection of subsets of U is a **partition** if every element of U is in exactly one of the subsets. For example, in the universe of letters,

$$V = \{\text{vowels}\} \text{ and } C = \{\text{consonents}\}$$

is a partition into two sets (let's agree that y is a consonent).

The two subsets of **even** and **odd** integers partition the integers:

$$\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$$

As another example, the three sets: $\mathbb{Z}^{<0}$, $\{0\}$, $\mathbb{Z}^{>0}$ of negative integers, zero and positive integers partition $\mathbb{Z}$. and a final example, the singleton sets $\{a\}$ for $a \in \mathbb{Z}$ partition $\mathbb{Z}$ into infinitely many subsets.

The **Cartesian product** of sets A and B is the set of ordered pairs:

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

Remarks. (a) The vertical slash means "such that," so the line reads: "$A \times B$ is the set of ordered pairs (a, b) such that a is an element of A and b is an element of B."

(b) If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.

Given a partition of U into (possibly infinitely many) subsets A, let:

$$x \sim y \text{ when } x, y \in A$$

belong to the same set A of the partition. This is the **equivalence relation** associated to the partition of U, and the sets of the partition are called the **equivalence classes.** Thus, for example, in the partition of $\mathbb{Z}$ into odd and even integers,

$$x \sim y \text{ when } x \text{ and } y \text{ are either both odd or both even integers}$$

In this example, we can describe the relation with a rule:

$$x \sim y \text{ when } x - y \text{ is even}$$

A **relation** on U is a subset of the Cartesian product:

$$R \subset U \times U \text{ with } x \sim y \text{ when } (x, y) \in R$$

For example, the subset:

$$R = \{(1, 1), (2, 1), (2, 2)\} \subset \{1, 2\} \times \{1, 2\}$$

is the relation $x \geq y$ on the universe $U = \{1, 2\}$.

A given relation R on a universe U is:

Reflexive if $x \sim x$ for all $x \in U$

Symmetric if $x \sim y$ implies that $y \sim x$.

Transitive if $x \sim y$ and $y \sim z$ imply that $x \sim z$.

For example, $x \geq y$ is not symmetric, but it is reflexive and transitive.

The relation associated to a partition satisfies all three properties. Conversely, any relation R that satisfies the three properties is called an **equivalence relation**, and it partitions U into **equivalence classes.** In other words, partitions and equivalence relations are the same thing!

Given an equivalence relation, such as the odd/even relation on $\mathbb{Z}$:

$$x \sim y \text{ if } x - y \text{ is even}$$

there is a conundrum, namely, what do we name the equivalence classes? One way to do this is by choosing a single element from each, and using the element to name the equivalence class. Thus, we could let:

$$[0] = \{\text{even integers}\} \text{ and } \ [1] = \{\text{odd integers}\}$$

This can be useful, but it has one drawback, which is that a single equivalence classes has as many names as it has elements. Thus:

$$..., [-4], -[2], [0], [2], [4], ... \text{ are all names for the even integers}$$

Next, we turn briefly to the question of **counting** elements of sets. Every finite set can be counted by a bijection from one of the sets:

$$A_1 = \{1\}, A_2 = \{1,2\}, A_3 = \{1,2,3\}, ..., A_n = \{1,2,3,...,n\}, ...$$

which are all subsets of the universe of natural numbers:

$$\mathbb{N} = \{1, 2, 3, ...\}$$

A bijection from $\mathbb{N}$ itself to a set S is an "infinite" count of S, and such a set is said to be **countable** or **countably infinite**.

Next, we consider the bijections from a finite set to **itself.**

Definition. A bijection from A_n to A_n is a **permutation** on n letters.

Remarks. (a) A permutation f on n letters is the list:

$$f(1), f(2), \ldots, f(n) \in A_n$$

of **distinct** values of f, and there are $n!$ ways to create this list:

$$n \text{ ways to choose } f(1) \text{ times } n-1 \text{ ways to choose } f(2), \text{ etc.}$$

(b) Because they are bijections from A_n to itself, permutations can be composed, and composing permutations has some interesting features.

Example. We can list all 6 permutations of A_3 in a table:

f	f_1	f_2	f_3	f_4	f_5	f_6
$f(1)$	1	1	2	2	3	3
$f(2)$	2	3	1	3	1	2
$f(3)$	3	2	3	1	2	1

Some immediate things to notice:

• The first permutation f_1 is the **identity** (do nothing) permutation.

• Each of the permutations f_2, f_3 and f_6 fix a single element and switch the other two. This means, in particular, that:

$$f_2 \circ f_2 = f_1,\ f_3 \circ f_3 = f_1 \text{ and } f_6 \circ f_6 = f_1$$

• The remaining pair of permutations cycle the elements of A_3, and:

$$f_4 \circ f_4 = f_5,\ f_4 \circ f_4 \circ f_4 = f_1,\ f_5 \circ f_5 = f_4 \text{ and } f_5 \circ f_5 \circ f_5 = f_1$$

We can capture the cycles of a permutation with **cycle notation**. In this notation, we "write out the cycles." So, for instance:

$(1\ 3\ 2)$ is the permutation that takes $f(1) = 3,\ f(3) = 2,\ f(2) = 1$

(the last value of f completes the cycle). Thus $(1\ 3\ 2) = f_5$.

$(1)(2\ 3)$ is the permutation that takes $f(1) = 1,\ f(2) = 3,\ f(3) = 2$

and comparing with the table above, we see that $(1)(2\ 3) = f_2$. Also:

$$(1)(2)(3) = f_1$$

and similarly, all the other permutations can be put in cycle notation.

Cycle notation is useful for **composing** permutations. For example:

$$f_5 \circ f_2 = (1\ 3\ 2) \circ (1)(2\ 3)$$

and we can use the cycle notation (reading right to left) to track:

$$1 \overset{f_2}{\mapsto} 1 \overset{f_5}{\mapsto} 3,\quad 3 \overset{f_2}{\mapsto} 2 \overset{f_5}{\mapsto} 1,\ 2 \overset{f_2}{\mapsto} 3 \overset{f_5}{\mapsto} 2$$

Putting this together, we get the cycle notation for the composition:

$$f_5 \circ f_2 = (1\ 3\ 2) \circ (1)(2\ 3) = (1\ 3)(2) = f_6$$

We will revisit this later in the course.

Exercises 1.1. The **power set** of A is the set of all subsets of A.

(a) What is the power set of the empty set?

(b) What is the power set of $A_1 = \{1\}$?

(c) What is the power set of A_2? of A_3?

(d) How many elements are there in the power set of A_n?

(e) Can you "see" Pascal's triangle in the elements of the power set?

1.2. Show that union and intersection satisfy both distributive laws:

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

and

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

(use a Venn diagram).

1.3. Justify the principle of inclusion and exclusion.

1.4. What are all the relations on $U = \{1, 2\}$? Which of them are equivalence relations?

1.5. Find cycle notation for each of the permutations $f_1, ..., f_6$.

1.6. Find a pair of permutations of A_3 that do **not** commute. That is, find a pair of permutations f_i and f_i so that:

$$f_i \circ f_j \neq f_j \circ f_i$$

1.7. Make a 6×6 "composition table" for $f_1, ..., f_6$.