6 First proofs: Elementary set theory[7]

As mathematicians and students of mathematics, it is our job to separate those mathematical assertions that are true from those that are false. The method that mathematicians use to verify that a mathematical assertion is true is called *deductive proof*. Roughly speaking, a deductive proof is a *step by step* argument that uses *known facts* and applies *valid rules of deduction* to build to a desired conclusion.

Theorems, propositions, corollaries, lemmas and conjectures We have been using the term *principle* to mean a mathematical assertion that has been proved to be true. Mathematicians usually label a principle as a *Theorem*, *Proposition*, *Lemma*, *Corollary* or *Claim*. These terms are not precisely defined but are used in the following way:

- A principle that is considered relatively important is called a *theorem*, otherwise it is called a *proposition*.
- A *corollary* refers to a a principle that is deduced as an easy consequence of a previously proved theorem.
- A *lemma* refers to a principle that is not so interesting by itself, but is of interest because it is a step in the proof of a theorem or a proposition. A relatively easy lemma may be called a *claim*.

An assertion for which there is no proof may be informally called a *speculative assertion*. If a mathematician believes that a speculative assertion is true based on some evidence (such as many successful test cases, or a partially completed proof), he might propose the assertion as a *conjecture*. There are a number of very interesting conjectures in mathematics that have not been proved yet. Conjectures are sometimes named by the person who proposed them. For example, one of the most famous conjectures in mathematics is *Goldbach's conjecture*:

> Every even number greater than 2 can be expressed as the sum of two primes.

It has been verified by computer that every even number between 4 and 4×10^{18} can be expressed as the sum of two primes. However, no one knows whether this is true of all even numbers.

First proof: An existential assertion Most theorems that mathematicians prove are universal principles, however sometimes they prove existential assertions. If a conjectured universal turns out to be false, then the counterexample yields an existential assertion. For example, suppose we had the following proposed universal principle:

Assertion 6.1. For any three sets A, B and C if $A \cap B \neq \emptyset$, $A \cap C \neq \emptyset$ and $B \cap C \neq \emptyset$ then $A \cap B \cap C \neq \emptyset$.

[7]Version: 2-11-2015.

It's not hard to see that this assertion is false. To prove it false you need to give a counterexample. A counterexample provides a proof of the negation of the above assertion, which is an existential assertion.

Proposition 6.1. *There exist sets A, B and C such that $A \cap B \neq \emptyset$, $A \cap C \neq \emptyset$ and $B \cap C \neq \emptyset$ and $A \cap B \cap C = \emptyset$.*

Proof. Let $A = \{1, 2\}$, $B = \{1, 3\}$ and $C = \{2, 3\}$. Then $A \cap B = \{1\}$, $A \cap C = \{2\}$ and $B \cap C = \{3\}$, while $A \cap B \cap C = \emptyset$. □

An existential assertion specifies a scenario, and to prove it we just need to show that there's at least one solution. Usually, this is done as above: we simply describe an example, and demonstrate that the example fits the scenario. However, this is not always easy; it may be very hard to come up with an example, or even if we have a proposed example, it may be very difficult to demonstrate that it has the needed properties.

Proving universal assertions: setting up the scenario Most of our efforts will be spent on proving universal principles. Such a principle has the form: "For all x of type T, if $A(x)$ then $C(x)$". As we've discussed, universal principles seem much more challenging to prove because a universal principle summarizes many assertions, one for every x of type T that satisfies $A(x)$. It is not enough to simply check a few examples of x's that satisfy $A(x)$. We need a way to simultaneously argue about all possible x's.

The proof of a universal principle *will always start* something like:

Suppose x is an arbitrary object of type T. Assume $A(x)$. We must show $C(x)$.

The first two sentences *set up the hypothetical scenario* for the universal principle. Having set up the hypothesis our goal is to show that the objects in the scenario satisfy the conclusion. This scenario and goal comprise the initial *proof task* to be accomplished.

The main part of the proof requires us to argue convincingly that $C(x)$ holds. Our argument may use the information about x given by the scenario (that x of type T and satisfies $A(x)$) but makes no other assumptions about x.

The scenario given by the object x satisfying $A(x)$ is the *starting scenario* of the proof and $C(x)$ is the *starting goal*, and together these comprise the *proof task* to be accomplished. As we'll see, as the proof proceeds the proof task will be modified. This modification involves both the scenario and the goal. We'll refer to this process as the *evolution of the proof task*. Understanding how this works is crucial to writing good proofs.

6.1 Proving universal principles in elementary set theory

The basic structure of proofs of universal principles is the same no matter what area of math you're working in. To get started with proofs we'll work in elementary set theory. We pick this area because:

- There are many examples of universal principles that are relatively easy to prove,

- The proofs illustrate many of the basic techniques of proof.
- The theorems proved, while easy, are useful in many areas of mathematics.

Before we actually start doing proofs, we need a starting point. This starting point consists of the basic definitions and facts about set theory. We introduced these in Section 2.1. We now carefully review and expand on these definitions in a more careful way.

In most settings, we are considering sets whoses members come from a particular *universe*. We denote the universe set by U. In what follows, S and T are arbitrary subsets of U and $(A_j : j \in J)$ is an indexed collection of sets of subsets from U.

Set membership For every set S and every object x, either x is a member of S, denoted $x \in S$ or x is not a member of S, denoted $x \notin S$.

Subset and superset For two sets S and T we say that S *is a subset of* T, denoted $S \subseteq T$, or T *is a superset of* S, denoted $T \supseteq S$ provided that for every $x \in S$, we have $x \in T$

Union The union of S and T, denoted $S \cup T$ is the set whose members are those x such that $x \in S$ or $x \in T$. The union of an indexed collection $(A_j : j \in J)$, denoted $\bigcup_{j \in J} A_j$, is the set consisting of those x such that there is a $j \in J$ with $x \in A_j$.

Intersection The intersection of S and T, denoted $S \cap T$ is the set whose members are those x such that $x \in S$ and $x \in T$. The intersection of indexed collection $(A_j : j \in J)$, denoted $\bigcap_{j \in J} A_j$, is the set consisting of those x such that for all $j \in J$, $x \in A_j$.

Set difference The difference between S and T, denoted $S \backslash T$ is the set of those x that belong to S but not to T.

Complement The complement of A is the set $U \backslash A$. (Notice that the definition of complement assumes that there is a fixed universe U. If we change the universe then the notion of complement may change. For example if A is the set of even integers and the universe is the set of integers then A^c is the set of odd integers, but if the universe is the set of real numbers then A^c is the union of the set of odd integers and the set of real numbers that are not integers.)

Symmetric Difference The symmetric difference of two sets A and B, denoted $A \triangle B$ is the set $A \backslash B \cup B \backslash A$.

Equality of Sets (biconditional version) Two sets S and T are equal provided that for every object x, $x \in S$ if and only if $x \in T$.

Equality of Sets (containment version) Two sets S and T are equal provided that $S \subseteq T$ and $T \subseteq S$.

Disjointness of sets Two sets A and B are disjoint provided that $A \cap B = \emptyset$. The collection $(A_j : j \in J)$ is disjoint if for any $i, j \in J$ with $i \neq j$ we have A_i and A_j are disjoint.

Here we are very careful to express these definitions precisely using the logical constructions (and, or, if-then, if and only if, there exists and for all) described in the earlier sections. For example, the condition that S is a subset of T is equivalent to the universal assertion that "for all $x \in S$ we have $x \in T$". (Note this is an indefinite assertion that depends on the free variables S and T, and that x is a dummy variable). Using this precise language sometimes makes the definitions seem more complicated, but is very useful as we start to prove things.

We will now state and prove some very simple universal principles. These principles are so simple as to be almost obvious, and they are easy to prove. Since the proofs are relatively easy, we'll be able to focus on expressing proofs in the proper form.

Proposition 6.2. *For any indexed collection of sets $(A_j : j \in J)$ and any $k \in J$ we have , $A_k \subseteq \bigcup_{j\in J} A_j$.*

Proof. Suppose $(A_j : j \in J)$ is an arbitrary indexed collection of sets and suppose k is an arbitrary member of J. We must show $A_k \subseteq \bigcup_{j\in J} A_j$. By definition of $\subseteq$ this means that we must show for every $x \in A_k$, we have $x \in \bigcup_{j\in J} A_j$. Suppose x is an arbitrary member of A_k. We must show $x \in \bigcup_{j\in J} A_j$. By the definition of the union, we must show that there is an index $i \in J$ such that $x \in A_i$. Since we assumed that $x \in A_k$, we have that k is an index in J that satisfies $x \in A_k$, which establishes that $x \in \bigcup_{j\in J} A_j$, as required. Since x was chosen to be an arbitrary member of A_k, we conclude $A_k \subseteq \bigcup_{j\in J} A_j$. □

Analysis of the proof. To analyze how this proof works, we need to understand the evolution of the proof task (scenario and goal). We go through the proof sentence by sentence.

- "Suppose $(A_j : j \in J)$ is an arbitrary indexed collection of sets and suppose k is an arbitrary member of J. We must show $A_k \subseteq \bigcup_{j\in J} A_j$." This sets up the starting proof task.

- "By definition of $\subseteq$ this means that we must show for every $x \in A_k$, we have $x \in \bigcup_{j\in J} A_j$." Here we used the definition of $\subseteq$ to replace the goal by an equivalent goal.

- "Suppose x is an arbitrary member of A_k." Since our goal is a "for all" statement we introduce a new object corresponding to the universal object in the goal. The object x enters our scenario.

- "We must show $x \in \bigcup_{j\in J} A_j$." Having introduced $x \in A_k$, the form of the goal becomes simpler.

- "By the definition of the union, we must show that there is an index $i \in J$ such that $x \in A_i$." Here we used the definition of the union of an indexed collection of sets to reformulate the goal: Show that "there is an index $i \in J$ such that $x \in A_i$"

- "Since we assumed $x \in A_k$, we have that k is an index in J that satisfies $x \in A_k$, so by definition $x \in \bigcup_{j\in J} A_j$, as required." We use the assumption in the scenario to achieve the current goal.

- "Since x was chosen to be an arbitrary member of A_k, we conclude $A_k \subseteq \bigcup_{j\in J} A_j$." We remind the reader that completing the current goal implies the original goal, and so completes the proof.

The reader should take note how, during the course of the proof, the proof task (scenario and goal) are modified several times. Each modification is driven by the current goal. This is what is meant by the *evolution of the proof task*.

Remark 6.1. This universal principle and most of the others in this section are easily visualized using the Venn Diagram picture. We are not satisfied with a picture because: (1) While pictures are helpful they can sometimes be misleading. (2) Our purpose is to practice doing careful and correct written proofs.

Remark 6.2. In this proof was most of the work was in modifying the goals and the scenario. Once we reached the new scenario and goal, achieving the goal was simple. The proofs in this section are similarly easy, to enable the student to master the crucial idea of the evolving scenario and goal.

Later on this course, the proofs will get more interesting; after modifying the scenario and the goal there will still be a lot of work to do.

Here are some additional propositions.

Proposition 6.3. *For all indexed collections of sets $(A_j : j \in J)$ and for all $k \in J$, $\cap_{j\in J} A_j \subseteq A_k$.*

Exercise 6.1. Prove Proposition 6.3

Corollary 6.4. *For any two sets A and B, $A \subseteq A \cup B$ and $A \cap B \subseteq A$.*

This is called a corollary because it follows easily by applying previously proved assertions.

Proof. Suppose that A and B are arbitrary sets. For the first conclusion, we want to apply Proposition 6.2. To do this we view (A, B) as an ordered pair of sets, so that it is an indexed collection. Then Proposition 6.2 implies $A \subseteq A \cup B$. Similarly Proposition 6.3 implies $A \cap B \subseteq A$. □

The next principle is called *transitivity of containment*.

Proposition 6.5. *For any three sets S,T, and U, if $S \subset T$ and $T \subset U$ then $S \subseteq U$.*

Proof. Suppose that S, T and U are arbitrary sets. Assume $S \subseteq T$ and $T \subseteq U$. We must show $S \subseteq U$. By definition, we must show that for all $x \in S$, we have $x \in U$. Suppose that $x \in S$. We must show $x \in U$. Since x is an arbitrary member of S and $S \subseteq T$ we have $x \in T$. Since $x \in T$ and $T \subseteq U$ we have $x \in U$, which is what we needed to show. Since x was an arbitrary member of S, $S \subseteq U$, as required to prove the proposition. □

The next principle shows that union and intersection satisfy a "distributive law".

Proposition 6.6. *For any indexed collection $(A_j : j \in J)$ of sets and any set B we have:*

1. $(\bigcup_{j\in J} A_j) \cap B = \bigcup_{j\in J}(A_j \cap B)$
2. $(\bigcap_{j\in J} A_j) \cup B = \bigcap_{j\in J}(A_j \cup B)$

Proof. The conclusion has two parts. We will show only the first part, and leave the second part as an exercise.

Suppose that $(A_j : j \in J)$ is an indexed collection of sets and suppose that B is a set. We must show:

$$(\bigcup_{j\in J} A_j) \cap B = \bigcup_{j\in J}(A_j \cap B),$$

which is equivalent to showing that for all x, $x \in (\bigcup_{j\in J} A_j) \cap B$ if and only if $x \in \bigcup_{j\in J}(A_j \cap B)$. So suppose x is an arbitrary object. We must show that $x \in (\bigcup_{j\in J} A_j) \cap B$ if and only if $\bigcup_{j\in J}(A_j \cap B)$.

Using one of the basic logical equivalences in Section 5 we see that the goal goal is logically equivalent to showing both of the following:

1. If $x \in (\bigcup_{j\in J} A_j) \cap B$ then $x \in \bigcup_{j\in J}(A_j \cap B)$
2. If $x \in \bigcup_{j\in J}(A_j \cap B)$ then $x \in (\bigcup_{j\in J} A_j) \cap B$.

We tackle the first goal first. Since our goal is an if-then, we assume the "if" part: $x \in (\bigcup_{j\in J} A_j) \cap B$. We must show $x \in \bigcup_{j\in J}(A_j \cap B)$. Since $x \in (\bigcup_{j\in J} A_j) \cap B$, we know that $x \in B$ and also $x \in \bigcup_{j\in J} A_j$. From the latter condition, we conclude that there is an index belonging to J that we'll call k such that $x \in A_k$. Then $x \in B \cap A_k$ which is a subset of $\bigcup_{j\in J}(A_j \cap B)$

For the second goal, we assume $x \in \bigcup_{j\in J}(A_j \cap B)$. We must show $x \in (\bigcup_{j\in J} A_j) \cap B$. By the assumption and the definition of union there is an index in J that we'll call p such that $x \in A_p \cap B$. Therefore $x \in A_p$ and $x \in B$. Since $x \in A_p$, we have also that $x \in \bigcup_{j\in J} A_j$ and so $x \in (\bigcup_{j\in J} A_j) \cap B$. □

Exercise 6.2. Prove the second part of Proposition 6.6.

Properties of disjointness

Proposition 6.7. *For all sets A,B,C and D, If A is disjioint from B and C is disjoint from D then $A \cap B$ is disjoint from $C \cup D$.*

Exercise 6.3. Prove Proposition 6.7.

Properties of set difference

Proposition 6.8. *For any four sets A,B, C, D we have:*

1. *$A\backslash B$ is disjoint from B.*
2. *$A\backslash B \subseteq A$.*

3. $A \backslash B = A \cap B^c$.

4. $(A \backslash B) \backslash C \subseteq A \backslash (B \cup C)$.

5. $(A \backslash B) \cap C = (A \cap C) \backslash B = (A \cap C) \backslash (B \cap C)$.

6. $(A \backslash B) \cup C = (A \cup C) \backslash (B \cup C)$

7. *If* $A \subseteq C$ *then* $D \subseteq B$ *then* $A \backslash B \subseteq C \backslash D$.

Exercise 6.4. Prove Proposition 6.8

Exercise 6.5. Here are some universal assertions that are similar to those in Proposition 6.8, but are actually false. Find counterexamples to theml.

- $(A \backslash B) \cup C = (A \cup C) \backslash B$.
- If $A \subseteq B$ and $C \subseteq D$ then $A \backslash C \subseteq B \backslash D$.

Properties of symmetric difference

Proposition 6.9. *For any two sets* A *and* B*, we have:*

1. $A \backslash B \subseteq A \triangle B$ *and* $B \backslash A \subseteq A \triangle B$.

2. $(A \cup B)^c$ *and* $A \cap B$ *are both disjoint from* $A \triangle B$.

Proof. Suppose that A and B are arbitrary sets.

For the first part, we must show $A \backslash B \subseteq A \triangle B$ and $B \backslash A \subseteq A \triangle B$. Since $A \triangle B$ is the union of the two sets $A \backslash B$ and $B \backslash A$, corollary 6.4 tells us that $A \triangle B$ is a superset of both of these sets.

For the second part we must show $(A \cup B)^c$ and $A \cap B$ are disjoint from $A \triangle B$. This is equivalent to showing the following two assertions: (1) if $x \in (A \cup B)^c$ then $x \notin A \triangle B$ and (2) if $x \in A \cap B$ then $x \notin A \triangle B$. For the first assertion, supoose x is an arbitrary member of $(A \cup B)^c$. Then $x \notin A$ and $x \notin B$. Since $x \notin A$, we have $x \notin A \backslash B$ and since $x \notin B$ we have $x \notin B \backslash A$. So $x \notin (A \backslash B) \cup (B \backslash A)$. For the second assertion, suppose x is an arbitrary member of $A \cap B$. Since $x \in A$, $x \notin B \backslash A$, and since $x \in B$, $x \notin A \backslash B$, so $x \notin (B \backslash A) \cup (A \backslash B)$, as required.

□

Proposition 6.10. *For any two sets* A *and* B*, and any object* x*, we have:*

1. *If* x *belongs to exactly one of the sets* A *and* B *then* $x \in A \triangle B$

2. *If* x *belongs to neither of* A *and* B*, or to both of* A *and* B*, then* $x \notin A \Delta B$.

Proof. Suppose A and B are arbitrary sets, and x an arbitrary object.

For the first part, assume that x belongs to exactly one of the sets A and B. We split into two cases depending on whether $x \in A$ or $x \in B$.

Case 1. Assume $x \in A$. Then $x \notin B$ (since x belongs to exactly one of the two sets). By definition of $A\backslash B$, $x \in A\backslash B$. By Proposition 6.9, $A\backslash B \subseteq A\triangle B$, so $x \in A\triangle B$.

Case 2. Assume $x \in B$. Then $x \notin A$ (since x belongs to exactly one of the two sets).2 By definition of $A\backslash B$, $x \in B\backslash A$. By Proposition 6.9, $B\backslash A \subseteq A\triangle B$, so $x \in A\triangle B$.

Since in either case, $x \in A\triangle B$, we conclude that $x \in A\triangle B$.

For the second part of the proposition, assume x belongs to one or both of the sets A and B.

□

Remark 6.3. This is our first example of *splitting a proof into cases*. In this situation we have deduced that $x \in A$ or $x \in B$. So we consider each of these possibilities separately as separate **cases**. In each case, we make an assumption, called the *case assumption*. We show that with this assumption the desired conclusion holds. Since at least one of the case assumptions must be true we may conclude holds.

Proposition 6.11. *For any sets A, B and C, we have:*

1. $A\triangle\emptyset = A$.
2. $(A\triangle B)\triangle C = A\triangle(B\triangle C)$.
3. $A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C)$.

Proof. We'll only prove the third part; the other two are left as exercises.

Suppose A, B and C are sets. We must show that $A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C)$. To simplify notation let L represent the set $A\cap(B\triangle C)$ and R represent the set $(A\cap B)\triangle(A\cap C)$. We must show that for all x, $x \in L$ if and only if $x \in R$. Suppose x is an arbitrary member of the universe. We must show $x \in L$ if and only if $x \in R$, which is logically equivalent to showing that either $x \in L$ and $x \in R$ or $x \notin L$ and $x \notin R$. We split the argument into two cases, depending on whether $x \in A$ or $x \notin A$.

Case 1. Assume $x \notin A$. Since each of the three sets $A\cap(B\triangle C)$, $A\cap B$ and $A\cap C$ is a subset of A, x belongs to none of these sets. Thus $x \notin L$ and since $x \notin A\cap B$ and $x \notin A\cap C$, Proposition 6.10 implies that $x \notin (A \cap B)\triangle(A \cap C)$ which is R. Thus $x \notin L$ and $x \notin R$, which completes this case.

Case 2. Assume $x \in A$. This implies that $x \in B$ if and only if $x \in A \cap B$ and $x \in C$ if and only if $x \in A \cap C$. Therefore the number of sets from A, B that x belongs to is equal to the number of sets from $A\cap B$ and $A\cap C$ that x belongs to. We split into two subcases, depending on whether x belongs to exactly one of the sets B and C, or not.

Subcase a. Assume x is in exactly one of the sets B and C. Then x also belongs to exactly one of the sets $A \cap B$ and $A \cap C$. By Proposition 6.9, $x \in B\triangle C$, and since $x \in A$, by definition of $\cap$, $x \in L$. Also, since x belongs to exactly one of the sets $A \cap B$ and $A \cap C$, by Proposition 6.9, $x \in (A \cap B)\triangle(A \cap C)$ and so $x \in R$. So $x \in L$ and $x \in R$ as required.

Subcase b. Assume x is in neither or both of the sets B and C. Then x belongs to neither or both of the sets $A \cap B$ and $A \cap C$. So by Proposition 6.9 $x \notin B \triangle C$, and so $x \notin L = A \cap (B \triangle C)$, and $x \notin R = (A \cap B) \triangle (A \cap C)$. So x is in neither L nor R as required. □

Exercise 6.6. 1. Prove part 2 of Proposition 6.11

2. Show that if we replace both occurrence of $\cap$ by $\cup$ in part 2 of Proposition 6.11, the resulting assertion is false.

Properties of the power set Recall that for a set A, $\mathcal{P}(A)$ is the set of all subsets of A.

Proposition 6.12. *For any two sets A and B, if $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}B$.*

Proof. Suppose A and B are sets. Assume $A \subseteq B$. We must show $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, which is equivalent to showing that for all $X \in \mathcal{P}(A)$ we miust have $X \in \mathcal{P}(B)$. Suppose $X \in \mathcal{P}(A)$. We must show $X \in \mathcal{P}(B)$. Since $x \in \mathcal{P}(A)$, by definition of the power set, $x \subseteq A$. Since $X \subseteq A$ and $A \subseteq B$, then by transitivity of containment $X \subseteq B$, and so by the definition of $\mathcal{P}(B)$ we have $x \in \mathcal{P}(B)$. Since X was an arbitrary member of $\mathcal{P}A$ we conclude $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. □

Remark 6.4. In this proof we used X instead of x as an arbitrary member of $\mathcal{P}(A)$. This is because members of $\mathcal{P}(A)$ are subsets of A, and it is conventional to represent subsets by capital letters.

Exercise 6.7. For each of the following two assertions, determine whether it's true. If it's true, prove it. If it's false, prove that its false.

1. For any two sets A and B, $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
2. For any two sets A and B, $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.
3. For any two sets A and B, $\mathcal{P}(A \cup B) \supset \mathcal{P}(A) \cup \mathcal{P}(B)$.
4. For any two sets A and B, $\mathcal{P}(A) \backslash \mathcal{P}(B) \subseteq \mathcal{P}(A \backslash B)$.
5. For any two sets A and B, $\mathcal{P}(A) \backslash \mathcal{P}(B) \supseteq \mathcal{P}(A \backslash B)$.

Properties of set products Recall that if A and B are sets then $A \times B$ denotes the set of all ordered pairs with first entry in A and second entry in B.

Proposition 6.13. *For all sets A,B,C and D we have:*

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. $A \times \emptyset = \emptyset$.
4. $(A \times B) \cap (D \times C) = (A \cap D) \times (B \cap C)$.

5. $(A \times B) \cup (D \times C) \subseteq (A \cup D) \times (B \cup C)$.

6. $(A \times B) \cup (D \times C) \supseteq (A \cup D) \times (B \cap C)$.

Proof. Suppose that A, B, C and D are arbitrary sets. There are several things to prove. We wll only consider the first, and leave the others as exercises

For the proof of the first part, we must show (i) $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ and also (ii) $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. For part (i) we must show that for every member of $A \times (B \cup C)$ is a member of $(A \times B) \cup (A \times C)$. Suppose that (a, b) is an arbitrary member of $A \times (B \cup C)$. We must show $(a, b) \in (A \times B) \cup (A \times C)$. Since $(a, b) \in A \times (B \cup C)$ we have $a \in A$ and $b \in B \cup C$. So we have $b \in B$ or $b \in C$. We consider these possibilities separately.
Case 1. Assume $b \in B$. Then $(a, b) \in A \times B$ and so $(a, b) \in (A \times B) \cup (A \times C)$, as required.
Case 2. Assume $b \in C$. Then $(a, b) \in A \times C$ and so $(a, b) \in (A \times B) \cup (A \times C)$.

Since (a, b) was an arbitrary member of $A \times (B \cup C)$ we conclude that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ which concludes part (i). Part (ii) is left as an exercise. □

Exercise 6.8. 1. Complete the proof of the first part of Proposition 6.13.

2. Prove parts 2-6 of Proposition 6.13

6.2 Elementary principles for functions

Interesting mathematics starts with interesting questions. In many parts of these notes we'll study some aspect of the mathematical universe, and we'll focus on some basic questions.

In this section we'll be looking at composition of functions. Recall that if $f : B \longrightarrow C$ and $g : A \longrightarrow B$ then $f \circ g$ is the function from A to C given by $f \circ g(a) = f(g(a))$.

- *When can a function be canceled from both sides of an equation?* One of the basic properties of addition of numbers is the cancellation property: For any three numbers a, b and c, if $a + b = a + c$ then $b = c$.

  Suppose three functions f, g and h satisfy $f \circ g = f \circ h$. Can we always cancel the f's and conclude $g = h$? If not, what properties of f allow us to do such a cancellation? A function f is called *left-cancellable* if this cancellation is always possible. We can ask a similar question for right cancellation: if $r \circ f = s \circ f$ what must be true about f to conclude that $r = s$?

- *Which functions have an inverse?* A *left inverse* for f is a function g such that $g \circ f$ is the identify function on $\mathbf{Dom}(f)$. Which functions f have a left inverse? Can f have more than one left inverse? If so, which functions have more than one left inverse and which functions have only one? Similarly, a right inverse for f is a function h so that $f \circ h$ is the identity on the target of f. When does f have a right inverse? When does f has more than one right inverse? Can f have a right inverse but no left inverse?

To investigate these questions, we start with some definitions.

Definition 6.1. function with target For some discussions of functions it is important that the functon come equipped with a target set that contains the range. We refer to this as a *function f with target T*. The notation $f : S \longrightarrow T$ means that f is a function with target T and domain S.

left cancellable A function f is said to be *left-cancellable* provided that for every pair of functions g and h with target set $\mathbf{Dom}(f)$, if $f \circ g = f \circ h$ then $g = h$.

right cancellable A function f with target set T is said to be *right-cancellable* provided that for every pair of functions g and h, if $\mathbf{Dom}(g) = \mathbf{Dom}(h) = T$ and $g \circ f = h \circ f$ then $g = h$.

right invertible A function f with target T is right-invertible provided that there is a function g with domain T such that $f \circ g = \mathbf{id}_T$.

one-to-one A function f is *one-to-one* (or *injective*) provided that for any $x_1, x_2 \in \mathbf{Dom}(f)$ if $f(x_1) = f(x_2)$ then $x = y$.

onto A function f with target T is *onto* (or *surjective*) provided that for all $y \in T$ there is an $x \in \mathbf{Dom}(f)$ such that $f(x) = y$.

bijection A function f with target T is a *bijection* if it is both one-to-one and onto.

Proposition 6.14. *Suppose $f : A \longrightarrow B$. Then $\mathbf{id}_B \circ f = f$ and $f \circ \mathbf{id}_A = f$.*

Exercise 6.9. Prove Proposition 6.14

The following theorem shows that the notions of left-cancellability, left invertibility and one-to-one are equivalent

Theorem 6.15. *For any function $f : A \longrightarrow B$ (with A nonempty), the following three properties of f are equivalent:*

1. *f is left-cancellable*
2. *f is left-invertible*
3. *f is one-to-one.*

Remark 6.5. This theorem is quite interesting. We start with three separate properties that a function might have. This theorem says that even though the definitions of the three properties are quite different, they are equivalent in the sense that a function that has any of them has all three of them.

When we want to prove equivalence of two conditions 1 and 2, we need to show that 1 implies 2, and also 2 implies 1. Here we need to show 6 things: 1 implies 2, 2 implies 1, 1 implies 3, 3 implies 1, 2 implies 3 and 3 implies 2. However, there is a short cut: if we order the conditions (in any order we like such as 3,2,1 then it is enough to prove that 1 implies 2, 2 implies 3 and 3 implies 1.

The other three implications follow "for free". For example once we know that 1 implies 2 and 2 implies 3, we can deduce that 1 implies 3.

Proof. Suppose $f : A \longrightarrow B$ with A nonempty. We must show that the three conditions in the conclusion are equivalent. We'll separately show 3 implies 2, 2 implies 1 and 1 implies 3.

Proof that 3 implies 2. Assume f is one-to-one. We must show that f is left-invertible, which means we need to construct a function $g : B \longrightarrow A$ such that $g \circ f = \mathbf{id}_A$. By the definition of $\mathbf{Rng}(f)$, for each $r \in \mathbf{Rng}(f)$ there is an element in $\mathbf{Dom}(f)$, which we'll call x_r such that $f(x_r) = r$. Since $A = \mathbf{Dom}(f)$ is nonempty, we can select an element from A, which we'll call z. Define $g : B \longrightarrow A$ by the rule $g(b) = x_b$ for $b \in \mathbf{Rng}(f)$ and $g(b) = z$ for $b \in B - \mathbf{Rng}(f)$. We now show that $g \circ f = \mathbf{id}_A$ which will show that g is a left-inverse for f.

The function $g \circ f$ and $\mathbf{id}_A$ both have domain A. We must show that for all $a \in A$, $g(f(a)) = a$. Let $b = f(a)$. Since $b \in \mathbf{Rng}(f)$, the definition of g implies that $g(b) = x_b$. We need to show that this is equal to a. By definition of x_b we have that $f(x_b) = b$ which is equal to $f(a)$. Since f is one-to-one, $x_b = a$. Therefore $g(f(a)) = g(b) = x_b = a$ as required. Since a is an arbitrary member of A, g is a left-inverse of f.

Proof that 2 implies 1. Assume f has a left inverse. We must show that f is left-cancellable. Using the definition of left-cancellable, we suppose that g and h are arbitrary functions having target A. Assume that $f \circ g = f \circ h$. We must show $g = h$. Since f is left-invertible there is a function $w : B \longrightarrow A$ so that $w \circ f = \mathbf{id}_A$. Since $f \circ g = f \circ h$, we have $w \circ f \circ g = w \circ f \circ h$. The first function is equal to $(w \circ f) \circ g = \mathbf{id}_A \circ g = g$ and the second function is equal to $(w \circ f) \circ h = \mathbf{id}_A \circ h = h$. Therefore $g = h$ as required.

Proof that 1 implies 3. The assertion that $1 \implies 3$ is logically equivalent to $(\neg 3) \implies (\neg 1)$. So we prove that if f is not one-to-one then f is not left-cancellable. Assume that f is not one-to-one. We'll find two different functions g and h with range A such that $f \circ g = f \circ h$, which will prove that f is not left cancellable. Since f is not one-to-one, there are two different domain elements a and a' such that $f(a) = f(a')$. Define g to be the function on domain $\{1\}$ such that $g(1) = a$ and h be the function on domain $\{1\}$ such that $h(1) = a'$. Then $f \circ g$ has domain $\{1\}$ and maps 1 to $f(a)$ and $f \circ h$ has domain $\{1\}$ and maps 1 to $f(a') = f(a)$. So $f \circ g = f \circ h$ but $g \neq h$ as required. □

There is a similar theorem for right-cancellability and right-invertibility.

Theorem 6.16. *For any function $f : A \longrightarrow B$ (with A nonempty), the following three properties of f are equivalent:*

1. *f is right-cancellable*
2. *f is right-invertible*
3. *$f : A \longrightarrow B$ is onto.*

Exercise 6.10. Prove Theorem 6.16

Exercise 6.11.

1. Give an example of a function $f : A \longrightarrow B$ that has a left-inverse but no right-inverse. Show that your example has at least two different left-inverses.
2. Give an example of a function $f : A \longrightarrow B$ that has a right-inverse but no left inverse. Show that your example has at least two different right-inverses.

The previous exercise shows that a function can have a left-inverse without having a right-inverse and that it can have more than one left-inverse and more than one right-inverse.

If the function happens to have both a left inverse and a right inverse, then the picture simplifies. We need some definitions.

Definition 6.2. Invertible function A function with target that is both left-invertible and right-invertible is said to be *invertible*

Proposition 6.17. *Any invertible function with target $f : A \longrightarrow B$ has a unique left-inverse and a unique-right inverse, and they are equal to each other.*

Proof. Suppose $f : A \longrightarrow B$ is a function with target. Assume that f has at least one left-inverse and at least one right-inverse. Let g be an arbitrary left inverse and h be an arbitrary right inverse. and h is a right-inverse of f.

First we show that $g = h$. Since $g : B \longrightarrow A$ and $h : B \longrightarrow A$, we can form the composition $f \circ h : A \longrightarrow A$ and $g \circ (f \circ h) : B \longrightarrow A$. Since h is a right-inverse of f, $f \circ h = \mathbf{id}_B$ and since g is a left-inverse of f, $g \circ f = \mathbf{id}_B$. Therefore:

$$g \circ (f \circ h) = g \circ \mathbf{id}_B = g.$$

Also

$$g \circ (f \circ h) = (g \circ f) \circ h = \mathbf{id}_B \circ h = h.$$

Therefore $g = h$.

Now since g was an arbitrary left-inverse, we have that any left-inverse must equal h so that any two left-inverses must be equal. Similarly, since h was an arbitrary right-inverse, any right-inverse must equal g and so any two right-inverses must be equal.

We conclude that if f has both a left-inverse and a right-inverse then it has a unique left-inverse and a unique-right inverse and they must be equal. □

Definition 6.3. inverse function An *inverse* of a function f is a function that is both a left-inverse and a right-inverse of f. By Proposition 6.17, the inverse of an invertible function f is unique. We denote the unique inverse of an invertible function f by f^{-1}.

Theorem 6.18. *Let $f : A \longrightarrow B$. The following conditions are equivalent:*

1. *f is invertible.*
2. *f is bijective*
3. *f has a unique left-inverse*
4. *f has a unique right-inverse*
5. *f is left-cancellable and right-cancellable*

Exercise 6.12. Prove Theorem 6.18

Theorem 6.19. *For any functions $g : A \longrightarrow B$ and $f : B \longrightarrow C$, we have that $f \circ g : A \longrightarrow C$ is well-defined and*

1. *If g_0 is a left-inverse of g and f_0 is a left-inverse of f then $g_0 \circ f_0$ is a well-defined function from C to A, and is a left-inverse of $f \circ g$. Thus if g and f are left-invertible so is $f \circ g$.*

2. *If g_0 is a right-inverse of g and f_0 is a right-inverse of f, then $f_0 \circ g_0$ is a well-defined function from C to A, and is a right-inverse of $f \circ g$. Thus if g and f are right-invertible so is $f \circ g$.*

3. *If g is invertible and f is invertible then so is $f \circ g$, and $(f \circ g)^{-1}$ is equal to $g^{-1} \circ f^{-1}$.*

Proof. Suppose that $g : A \longrightarrow B$ and $f : B \longrightarrow C$ are functions with target. Then $f \circ g$ is a well-defined function from A to C since for any $a \in A$ $f(a)$ is defined and belongs to B and so $g(f(a)) \in C$.

For the first numbered part, suppose that g_0 is a left-inverse of g and that f_0 is a left-inverse of f. Then $g_0 : B \longrightarrow A$ and $f_0 : C \longrightarrow B$. Since $B = \mathbf{Dom}(g_0)$ is equal to the target of f_0, and $\mathbf{Dom}(f_0) = C$ and the function $g_0 \circ f_0$ is a well-defined function from C to A. We claim that it is a left-inverse of $f \circ g$. Using the fact that composition of functions is associative, we have:

$$(g_0 \circ f_0) \circ (f \circ g) = g_0 \circ ((f_0 \circ f) \circ g) = g_0 \circ ((\mathbf{id}_A \circ g) = g_0 \circ g = \mathbf{id}_A,$$

as required.

The second part is similar to the first part and is left as an exercise.

For the third part, assume that g is invertible and f is invertible. Then by definition of invertible, g^{-1} and f^{-1} are left-inverses of g and f, respectively, and so $g^{-1} \circ f^{-1}$ is a left-inverse of $f \circ g$. Also, by definition of invertible, g^{-1} and f^{-1} are right-inverses of g and f, respectively, and so $g^{-1} \circ f^{-1}$ is a right-inverse of $f \circ g$. Since $g^{-1} \circ f^{-1}$ is both a left-inverse and a right-inverse of $f \circ g$, it is an inverse of $f \circ g$ and so $f \circ g$ is invertible and $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. □

Remark 6.6. It is important to notice that when we take the inverse of $f \circ g$, the inverses of f and g are composed in the opposite order $g^{-1} \circ f^{-1}$. Composing them in the order $f^{-1} \circ g^{-1}$ will not work. In fact $f^{-1} \circ g^{-1}$ is not well-defined in general since since the target A of g^{-1} doesn't agree with the domain C of f^{-1}.

Theorem 6.19 can be used to obtain the following:

Corollary 6.20. *For any functions $g : A \longrightarrow B$ and $f : B \longrightarrow C$,*

1. *If g is one-to-one and f is one-to-one then so is $f \circ g$.*

2. *If g is onto and f is onto then so is $f \circ g$.*

3. *If g is a bijection and f is a bijection then so is $f \circ g$.*

Proof. Suppose $g : A \longrightarrow B$ and $f : B \longrightarrow C$.

For the first part, assume that g is one-to-one and f is one-to-one. By Theorem 6.15 g and f are both left-invertible, and so by the first part of Theorem 6.19 $f \circ g$ is left-invertible and so by Theorem 6.15, $f \circ g$ is one-to-one.

The second and third parts are similar, and are left as exercises. □

Exercise 6.13. Prove the second and third parts of Corollary 6.20

Corollary 6.20 can be proved without using Theorems 6.19, 6.15, and 6.16. Instead you can directly apply the definition of one-to-one and onto. We'll show how to do this for part 2.

Proof. (Alternative proof of Corollary 6.20, part 2.) Suppose that $g : A \longrightarrow B$ and $f : B \longrightarrow A$. Assume that g is onto and that f is onto. We must show that $f \circ g$ is onto, which means that we must show that for every $c \in C$ there is an $a \in A$ such that $f \circ g(a) = c$. Suppose that c is an arbitrary member of C. We must show that there is an $a \in A$ such that $f \circ g(a) = c$. To do this, we need to describe a way to obtain such an a. Since f is onto, there is a $b \in B$ such that $f(b) = c$. Let b be such a member of B. Since g is onto there is an $a \in A$ such that $g(a) = b$. Let a be such a member of A.

We claim that $f \circ g(a) = c$. We have $f \circ g(a) = f(g(a))$ which equals $f(b)$ by the choice of a, and $f(b) = c$ by the choice of c. Thus $f \circ g(a) = c$, as required.

Since $c \in C$ was arbitrary, and we found $a \in A$ so that $f \circ g(a) = c$ □

Remark 6.7. This is our first example of an extremely important type of proof. When we try to prove that $f \circ g$ (or any function) is onto, we need to show that "For any $c \in C$, there is an $a \in A$ such that $f \circ g(a) = c$. " This is an example of a $\forall\exists$ type of assertion.

After we introduced c our goal was to show that there is an $a \in A$ such that $f \circ g(a) = c$. The choice of a depends on various things in the scenario: c, f and g. In order to prove this, we have to do two things: provide specific instructions for finding such an a, and then verify that the a we found has the required properties.

Notice that the introduction of a to the scenario is very different from the way c was introduced. We introduced c because we had a goal which was a universal assertion. So we introduced c to stand for an arbitrary member of C.

When we introduced a our goal was an existential assertion, and we need a to satisfy some specific properties. So we don't want a to be an arbitrary member of A, but rather a member of a carefully chosen to satisfy the properties we needed. Once we gave instructions for a we introduced it to the scenario with the sentence "Let a be such a member of a".

Assertions with $\forall\exists$ structure are extremely important in mathematics, and the proofs typically follow the above pattern. We'll see this type of proof many times throughout these notes.

Exercise 6.14. Give a different proof of Corollary 6.20, part 1 that does not use Theorems 6.19, 6.15, and 6.16 but instead apply the definition of one-to-one.