Proofs

Joshua Meyers

May 26, 2017

This document is intended to state the "rules" of mathematical proofs for Russell Dale.

1 Preliminaries

I will not define "set" or "element", as these are primitive notions.

Primitive Notion 1. *Set*

Primitive Notion 2. *Element. For a set S, $x \in S$ denotes that x is an element of S.*

I will also assume predicate logic, since I know you know that.
For convenience we define the negation of $\in$:

Definition 1. *For a set S, $s \notin S$ iff $\sim x \in S$*

2 The Axiom of Extention

Here is our first axiom:

Axiom 1.0 (Axiom of extension)**.** *For sets S and T, $S = T$ iff S and T have all the same elements.*

The axiom of extension is basically an admission that "set" is a concept of universal that is purely extensional. Version 1.1 makes this clear:

Axiom 1.1 (Axiom of extension)**.** *For sets S and T, $S = T$ iff S and T have the same extension.*

We can also rephrase the axiom of extension in terms of the $\in$ relation. This makes precise what we mean by "having all the same elements".

Axiom 1.2 (Axiom of Extension)**.** *For sets A and B, $A = B$ iff $(\forall x)(x \in A \Leftrightarrow x \in B)$.*

This form is more useful because it only uses our primitive notions and logic. It is useful for proving that two sets are equal. To prove that $A = B$, we must show that the property $x \in A$ is equivalent to the property $x \in B$.

Example 1. *Let $A = \{2k + 1 | k \in \mathbb{Z}\}$ and $B = \{2k - 1 | k \in \mathbb{Z}\}$. We show that $A = B$ by showing that $x \in A \Leftrightarrow x \in B$. First suppose that $x \in A$. Then $\exists k$ such that $x = 2k + 1$. We use existential instantiation to remove the quantifier and obtain $x = 2k + 1$. Now by algebra we obtain $x = 2(k + 1) - 1$, so by existential generalization, $\exists j$ such that $x = 2k - 1$, so $x \in B$. Thus $x \in A \Rightarrow x \in B$. By a similar argument, we can show that $x \in B \Rightarrow x \in A$. Thus $x \in A \Leftrightarrow x \in B$. By the axiom of extension, $A = B$.*

Now we define subsets. We denote "A is a subset of B" by $A \subseteq B$ and "A is not a subset of B" by $A \nsubseteq B$. We denote "A is a superset of B" by $A \supseteq B$ and "A is not a superset of B" by $A \not\supseteq B$,

Definition 2. *For sets A and B,*

a) $A \subseteq B$ iff $(\forall x)(x \in A \Rightarrow x \in B)$

b) $A \nsubseteq B$ iff $\sim A \subseteq B$

c) $A \supseteq B$ iff $B \subseteq A$

d) $A \not\supseteq B$ iff $\sim A \supseteq B$

The usual approach to prove that $A \subseteq B$ is to use a direct proof to show that for an arbirary x, $x \in A \Rightarrow x \in B$. So we start by supposing that $x \in A$, and we show from that that $x \in B$. We conclude that $(\forall x)(x \in A \Rightarrow x \in B)$, which is the definition of $A \subseteq B$.

Example 2. *Let A be the set of all multiples of 4, and B be the set of all multiples of 2. We want to show that $A \subseteq B$. Suppose $x \in A$. Then x is a multiple of 4, so there is an integer k such that $x = 4k$. But then $x = 2(2k)$, so x is a multiple of 2 and $x \in B$. So $x \in A \Rightarrow x \in B$, which is equivalent to $A \subseteq B$.*

A useful method for proving that two sets are equal is to prove that they are subsets of each other. This method is based on the truth of the following theorem:

Theorem 1. *For sets A and B, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.*

Proof.

$$\begin{aligned} A = B &\Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B) \\ &\Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A) \\ &\Leftrightarrow ((\forall x)(x \in A \Rightarrow x \in B) \wedge (\forall x)(x \in B \Rightarrow x \in A)) \\ &\Leftrightarrow (A \subseteq B \wedge B \subseteq A) \end{aligned}$$

The first equivalence comes from Axiom 1.2, the second and third come from logic, and the fourth comes from Def. 2. □

So it seems that we are building a correspondence between set theory and logic, so that we can prove things about sets using facts from logic. Axiom 1.2 expresses equality of sets in terms of equivalence of predicates. Def. 2 defines the subset relation in terms of the material conditional. In general, statements about sets reduce to statements about logic.

3 The "Axiom" of Comprehension

Now we need an axiom that can help us make sets.

Axiom 2.0 ("Axiom" of Comprehension)**.** *For a predicate P, there exists a set S such that $x \in S$ iff Px. The set S is then denoted $\{x|Px\}$.*

This "axiom" is not really an axiom, because it implies Russell's Paradox. Still, if we avoid Russell's paradox, it is sufficient for most purposes. We will use it for now and bracket the issue that it does not really work.

Before Axiom 2.0, we could go from a set S to the predicate $x \in S$, which is easier to work with. Now that we have Axiom 2.0, we can go the other way, from a predicate P to the set $\{x|Px\}$. So now we can go both says, from sets to predicates and from predicates to sets. Sets and predicates arguably contain the same information. The mathematical jargon for a change of data type that preserves the information is "induce". So we say that a set S *induces* the predicate $x \in S$ and a predicate P *induces* the set $\{x|Px\}$.

Now we define the null set, using the "axiom" of comprehension.

Definition 3. $\emptyset = \{x | x \neq x\}$

We have just defined the empty set as the set induced by the predicate $x \neq x$, which is never true. Since the predicate is never true, the set it induces has no elements. But we could have used a different contradictory predicate, such as "1=0" (This doesn't mention x, but it doesn't have to. It is possible for a predicate can ignore its argument completely.) Why didn't we define the null set as $x|1 = 0$? Would it have come out any different? The following theorem answers this question:

Theorem 2. *The null set is unique. In other words, if P is a contradictory predicate, then $\{x|Px\} = \emptyset$.*

Proof. Suppose P is a contradictory predicate. We will use Theorem 1 to prove that $\{x|Px\}$ and $\emptyset$ are equal by proving first that they are subsets of each other. First we prove that $\{x|Px\} \subseteq \emptyset$. Suppose that $\{x|Px\} \not\subseteq \emptyset$. Then $\exists x$ such that $x \in \{x|Px\}$ and $x \notin \emptyset$, which implies that Px, a contradiction. So $\{x|Px\} \subseteq \emptyset$. We can prove that $\emptyset \subseteq \{x|Px\}$ by a similar argument. Thus $\{x|Px\} = \emptyset$. □

This is a great illustration of the extensionality of the concept of set. Noah Schweber writes in a comment on StackExchange:

> I think proving that the emptyset is unique is a good piece towards demonstrating the extensionality, rather than intensionality, of set theory. The emptyset is possibly the most natural set given to lots of different intensional definitions: the set of counterexamples to Fermat and the set of primes with rational square roots are each the empty set, but clearly are different definitions. And for whatever reason, it's the set which seems to cause the most trouble in this regard. As trivial as it is, using the axiom of extensionality here plants the seed of extensional thinking.

4 Some More Theorems

Now I will state some more theorems without proof that can be proved with this same method: convert the statement about sets to a statement about the induced predicates and then use logic.

Theorem 3. *For a set A,*

a) $\emptyset \subseteq A$

b) $A \subseteq A$

Theorem 4. *The subset relation is a poset. In other words, for sets A, B, and C,*

a) $A \subseteq A$ *(reflexivity)*

b) $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$ *(antisymmetry)*

c) $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$ *(transitivity)*

We now define intersection and union in terms of logical operations on the induced predicates.

Definition 4. *For sets A and B, the union $A \cup B = \{x | x \in A \vee x \in B\}$ and the intersection $A \cap B = \{x | x \in A \wedge x \in B\}$.*

The following set-theoretic identities can all be proved from the corresponding logical laws obtained from replacing $\cup$ with $\vee$ and $\cap$ with $\wedge$.

Theorem 5. *The operations $\cup$ and $\cap$ are commutative, associative, and idempotent, and each distributes over the other. In other words, for sets A, B, and C,*

a) $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$

b) $A \cup (B \cup C) = (A \cup B) \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C$

c) $A \cup A = A$ *and* $A \cap A = A$

d) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *and* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof. We will prove just the distributivity of union over intersection (the first part of item d)) and leave the rest unproved. We prove the equality of $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$ through 1.2.

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow (x \in A) \vee (x \in B \cap C) \\ &\Leftrightarrow (x \in A) \vee (x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C) \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C) \end{aligned}$$

□

So far we have a set-theoretic relation $\subseteq$, which makes sets into a poset (cf. Thm. 4, and two set-theoretic operators, $\cup$ and $\cap$. It turns out that these operators have a special place with respect to the poset, as shown in the following theorem.

Theorem 6. *For sets A and B,*

a) $A \cup B$ is the least upper bound of A and B with respect to the $\subseteq$ ordering. In other words, $A \cup B \supseteq A, B$ (it is an upper bound of A and B) and for any set C, $C \supseteq A, B$ implies that $C \supset eq A \cup B$ (it is a subset of any upper bound of A and B). (Notice that we have used $\supseteq$, not $\subseteq$ here, so that it looks similar to part b).)

b) $A \cap B$ is the greatest lower bound of A and B with respect to the $\subseteq$ ordering. In other words, $A \cap B \subseteq A, B$ and for any set C, $C \subseteq A, B$ implies that $A \cap B \subseteq C$.

Proof. a) First we will prove that $A \cup B \supseteq A, B$. If $x \in A$, then by disjunction introduction $x \in A \vee x \in B$, so $x \in A \cup B$. Thus $A \subseteq A \cup B$. By a similar argument, $B \subseteq A \cup B$. Second we will prove that for any set C such that $A, B \subseteq C$, $A \cup B \subseteq C$. Suppose that C is a set and $A, B \subseteq C$. If $x \in A \cup B$, then $x \in A \vee x \in B$. Either disjunct of this last statement implies that $x \in C$, so by disjunction elimination, $x \in C$.

b) This second part of the theorem can be proved in a similar way to the first part, but with everything reversed. We would replace $\supseteq$ with $\subseteq$, $\cup$ with $\cap$, etc.

□

This theorem means that it would have been possible to define intersection and union just in terms of the subset relation, without any recourse to logic (though in this scenario, the subset relation itself would still be defined in terms of logic).

We also have a theorem that goes the other way, which would allow us (if we wanted) to define the subset relation just in terms of either union or intersection, with no recourse to logic (but in this case, union or intersection would have to be defined with logic). Here it is:

Theorem 7. *For sets A and B,*

a) $A \subseteq B$ iff $A \cup B = B$

b) $A \subseteq B$ *iff* $A = A \cap B$

Proof. a) We will prove each direction of the biconditional separately.

⇒) Suppose $A \subseteq B$. We prove $A \cup B = B$ by proving that $A \cup B \supseteq B$ and $A \cup B \subseteq B$. If $x \in B$, then $x \in A \vee x \in B$ by disjunction introduction, so $x \in A \cup B$. Thus $A \cup B \supseteq B$. And if $x \in A \cup B$, then either $x \in A$ or $x \in B$. In the first case, $x \in B$ by our supposition. In the second case, $x \in B$ by reiteration. Thus $x \in B$. So $A \cup B \subseteq B$.

⇐) Suppose $A \cup B = B$. We will prove that $A \subseteq B$ using the definition of $\subseteq$. Suppose $x \in A$. Then $x \in A \vee x \in B$, so $x \in A \cup B$. By our supposition, $x \in B$.

b) The second part is similar to the first.

□

5 DeMorgan's Laws

So far we have seen the set-theoretic analogues of many laws of logic. How about DeMorgan's Laws? Well, we need an analogue of negation first for that.

Definition 5. *For a set A, define its complement* $\overline{A} = \{x | x \notin A\}$.

The complement of A is the set of everything not in A. It is the set induced by the negation of the predicate which induces A.

Now we can state the set-theoretic analogue of DeMorgan's laws:

Theorem 8. *For sets A and B,*

a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

b) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Recall that a lot of our proofs above had two parts with similar proofs. DeMorgan's Law often let's us prove one of these parts from the other. For example, let's say that we know that union is distributive over intersection (as proved above), but not *vice versa* (as omitted above). We can prove the one from the other:

Proof. We know from the partial proof of Thm. 5 that for sets A, B, and C, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Now we substitute $\overline{A}$ for A, $\overline{B}$ for B, and $\overline{C}$ for C to obtain $\overline{A} \cup (\overline{B} \cap \overline{C}) = (\overline{A} \cup \overline{B}) \cap (\overline{A} \cup \overline{C})$. Then by DeMorgan's Laws,

$$\begin{aligned}
\overline{A} \cup (\overline{B} \cap \overline{C}) &= (\overline{A} \cup \overline{B}) \cap (\overline{A} \cup \overline{C}) \\
\overline{A} \cup \overline{B \cup C} &= \overline{A \cap B} \cap \overline{A \cap C} \\
\overline{A \cap (B \cup C)} &= \overline{(A \cap B) \cup (A \cap C)} \\
\overline{\overline{A \cap (B \cup C)}} &= \overline{\overline{(A \cap B) \cup (A \cap C)}} \\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C)
\end{aligned}$$

In the second-to-last step, we took the complement of both sides, and then in the last step, we used the fact that $\overline{\overline{S}} = S$. This fact can be proved from the corresponding logical law $\sim\sim P \Leftrightarrow P$. □