MATH 2135 Linear Algebra

Proofs

Alyssa Motas

April 12, 2021

Contents

1 What is a proof?

A proof is *evidence* for the validity of a theorem. This evidence is subject to very *strict* rules. Your first task is to learn threse rules, then you should be able to tell the difference between a proof and a non-proof. Your next task is to get good at proving things.

1. The goal of a proof is to show that a given *conclusion* follows from given *assumptions*.

   Example: "Every spanning list in a vector space can be reduced to a basis of the vector space." This statement is an English description of the following more precise statements:

   Assumptions/"Hypotheses:"

   - Let F be a field.
   - Let V be a vector space over F.
   - Let $v_1, \ldots, v_n$ be a list of elements of V.

   Conclusion:

   - If $v_1, \ldots, v_n$ is spanning, then $v_1, \ldots, v_n$ can be reduced to a basis of V.

   Our goal is to show that the conclusion follows from the assumptions.

2. In the course of proving things, the assumptions and conclusion can change. We will see examples of this.

3. To do any proof, we first need to understand what kind of statement the conclusion is. There are several different kinds of statements:

   - "and statement" or "conjunction:" "n is an odd prime" $\Leftrightarrow$ "n is odd and n is prime."
   - "or statement" or "disjunction:" "n is even or odd" $\Leftrightarrow$ "n is even or n is odd."
   - "if-then statement" or "implication:" "if $v_1, \ldots, v_n$ is spanning, then $v_1, \ldots, v_n$ can be reduced to a basis of V."
   - "not statements" or "negation:" "n is not prime."

- "for all statement" or "universally quantified statement:" "Every basis is linearly independent" $\Leftrightarrow$ "For all lists $v_1, \ldots, v_n$ of vectors, (if $v_1, \ldots, v_n$ is a basis, then $v_1, \ldots, v_n$ is linearly independent)."
- "exists statement" or "existentially quantified statement:" "There is an odd prime."

Note: The reason "if and only if" is not in the above list of statement types is that it is actually an "and statement." We treat "$A \Leftrightarrow B$" as an abbreviation of "$A \Rightarrow B$ and $B \Rightarrow A$."

2 Proof rules

Type of conclusion:	To prove:	You should do the following:
Conjunction	A and B	First we prove A. [Prove A] Next, we prove B. [Prove B] So we proved A and B, as required.
Implication	A implies B	Assume A. [Prove B] Since we assumed A, this proves that A implies B.
For all-statement	$\forall x \in A, P(x)$	Take an arbitrary $x \in A$. [Prove $P(x)$] Since x was arbitrary, this proves $\forall x \in A, P(x)$.
Not-statement	not A	Assume A. [Prove a contradiction]
Or-statement	A or B	<u>Method 1:</u> [Prove A]. Since we proved A, we have A or B. <u>Method 2:</u> [Prove B]. Since we proved B, we have A or B. <u>Method 3:</u> Assume that both A and B are false. [Prove a contradiction]
Exists-statement	$\exists x \in A, P(x)$	[Describe a specific element $a \in A$] [Prove $P(a)$]

3 Proof rules for using an assumption

Type of assumption:	If you already know:	You may use it as follows:
And-statement	A and B	You may conclude A. You may conclude B.
Or-statement	A or B	[Can proceed by case distinction] Case 1: A is true. [Prove the conclusion] Case 2: B is true. [Prove the conclusion]
Implication	$A \Rightarrow B$	Method 1: [If you also know A, you may conclude B] Method 2: [If you also know not B, then you may conclude not A]
Not-statement	not A	[If you also know A, you may derive a contradiction]
For all-statement	$\forall x \in A, P(x)$	[Given any element $a \in A$, you may conclude $P(a)$]
Exists-statement	$\exists x \in A, P(x)$	[You may give a new name to an unknown element $b \in A$. You may assume $P(b)$ holds]

4 Examples

1. Prove: For all sets A, B, C, we have

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

Proof. Let A, B, C be arbitrary sets. We msut show $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$. By definition of equality of sets, we must show

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

and

$$(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C.$$

We first prove $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$. We have to show $\forall x\, in (A \cup B) \cap C, x \in (A \cap C) \cup (B \cap C)$. Take an arbitrary $x \in (A \cup B) \cap C$ and we want to show $x \in (A \cap C) \cup (B \cap C)$. Equivalently, by definition of union, we must show $x \in A \cap C$ or $x \in B \cap C$.

Assumption 2 says: $x \in (A \cup B) \cap C$. By definition of intersection, we have $x \in A \cup B$ and $x \in C$. We conclude $x \in A \cup B$. We conclude $x \in C$.

The other inclusion is the same. Hence, we proved the statement provided. $\square$