MAT 3343, APPLIED ALGEBRA, FALL 2003

Handout 1: What is a proof?

This handout summarizes some basic techniques used in "everyday" proofs. We use the usual logical notations $P \wedge Q$ for "P and Q", $P \vee Q$ for "P or Q", $P \Rightarrow Q$ for "P implies Q", $\neg P$ for "not P", $\forall x \in A.P(x)$ for "for all $x \in A$, $P(x)$", $\exists x \in A.P(x)$ for "there exists an $x \in A$ such that $P(x)$".,

There are certain patterns that occur over and over in mathematical proofs; for instance, to prove a statement of the form $\forall x \in A.P(x)$, we have to take an arbitrary $x \in A$ and then prove $P(x)$. To prove $P \Rightarrow Q$, we assume P and then prove Q. The following table summarizes some phrases and formulations that are commonly used in proofs. The parts in [*brackets*] must be filled in.

To prove:		you might write the following:
$P \Rightarrow Q$		Assume P. [*Prove* Q]. Since we assumed P, this proves $P \Rightarrow Q$.
	Or:	Assume $\neg Q$. [*Prove* $\neg P$]. We have proved $\neg Q \Rightarrow \neg P$, which, by taking the contrapositive, implies $P \Rightarrow Q$.
$P \wedge Q$		First we prove P. [*Prove* P]. Then we prove Q. [*Prove* Q].
$\forall x \in A.P(x)$		Take an arbitrary $x \in A$. [*Prove* $P(x)$]. Since x was arbitrary, this proves $\forall x \in A.P(x)$.
$\neg P$		Assume P. [*Derive a contradiction*]. The assumption P led to a contradiction, therefore we have shown $\neg P$.
$\exists x \in A.P(x)$		[*Construct an object* a]. [*Prove* $P(a)$].
$P \vee Q$		[*Prove* P]. This implies $P \vee Q$.
	Or:	[*Prove* Q]. This implies $P \vee Q$.
	Or:	By contradiction: Assume neither P nor Q holds. [*Derive a contradiction*]. Therefore, either P or Q must be true.
	Or:	If P holds, we are done. So assume $\neg P$. [*Prove* Q]. Therefore $P \vee Q$.

(continued on the next page)

To prove:	you might write the following:
P (by contradiction)	Assume $\neg P$. [*Derive a contradiction*]. The assumption $\neg P$ led to a contradiction, thus we have proved P.
P (by case distinction)	(Here, Q is some statement). We distinguish two cases. Case 1: Q holds. [*Prove* P]. Case 2: $\neg Q$ holds. [*Prove* P]. In either case, we have proved P.
(to divide a long proof)	We will first show P. [*Show* P]. We have shown P. (etc.)

Another question is how you can *use* assumptions, hypotheses, axioms, and previously proved statements.

The statement:	can be used as follows:
$P \Rightarrow Q$	If you know P, you may conclude Q.
$P \wedge Q$	You may use P. You many also use Q.
$\forall x \in A.P(x)$	If you know $x \in A$, you may conclude $P(x)$.
$\neg P \wedge P$	This is a contradiction. Use it to conclude that the most recent assumption was false.
$\exists x \in A.P(x)$	You may conclude $P(b)$, for some *unknown* element $b \in A$. (You cannot choose b).
$P \vee Q$	You can use this in a case distinction. Suppose you are in the process of proving some statement C. Case 1: Assume P. [*Prove* C]. Case 2: Assume Q. [*Prove* C]. Then you know C is true.
$a = b$	If you know $P(a)$, you may conclude $P(b)$.

Here are a few more useful patterns, some from set theory.

To prove:	you have to show:
$P \Leftrightarrow Q$	$P \Rightarrow Q$ and $Q \Rightarrow P$.
$A \subseteq B$	For all $x \in A$, we must show that $x \in B$.
$A = B$ (for sets)	$A \subseteq B$ and $B \subseteq A$.
$x \in A \cap B$	$x \in A$ and $x \in B$.
$x \in A \cup B$	$x \in A$ or $x \in B$.