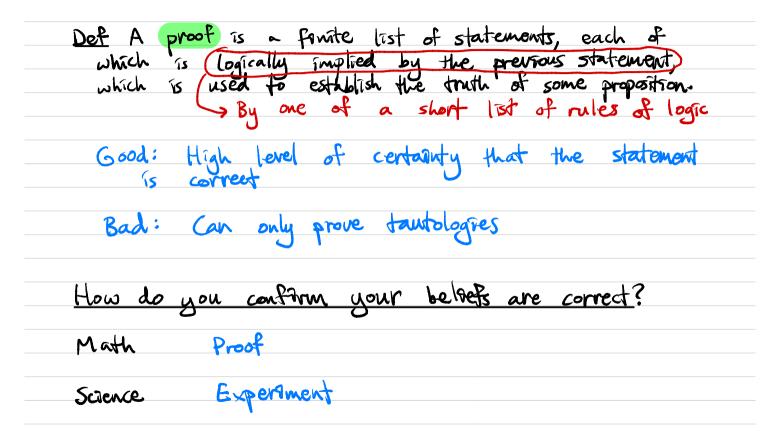
D Proofs

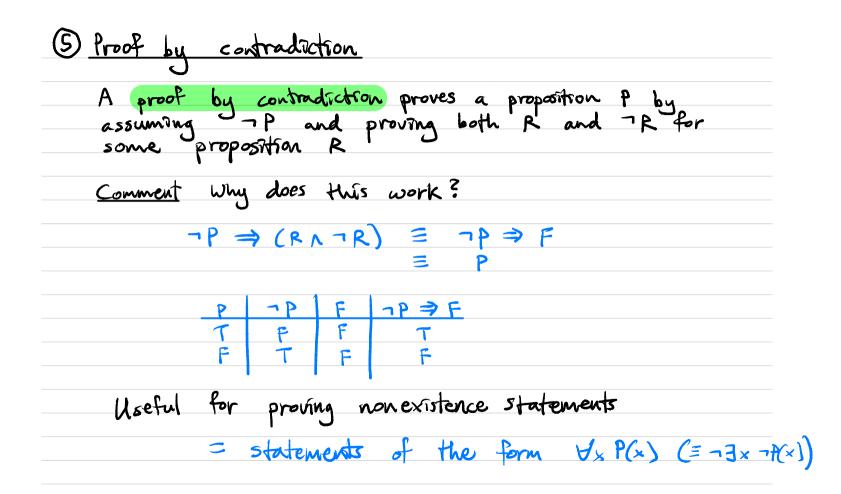


Def A proof is a finite list of statements, each of which is logically implied by the previous statement, which is used to establish the truth of some proposition. Not really! Proofs are written for humans.

 226	theorem nat_abs_add_le (a b : \mathbb{Z}) : nat_abs (a + b) \leq nat_abs a + nat_abs b :=	
227	begin	-> A formal proof
 228	have : \forall (a b : \mathbb{N}), nat_abs (sub_nat_nat a (nat.succ b)) \leq nat.succ (a + b),	
 229	{ refine (λ a b : ℕ, sub_nat_nat_elim a b.succ	written using the
230	$(\lambda m n i, n = b.succ \rightarrow nat_abs i \leq (m + b).succ) rfl);$	Lean proof assistant
 231	intros i n e,	Lean proot assistant
232	{ subst e, rw [add_comm _ i, add_assoc],	
 233	exact nat.le_add_right i (b.succ + b).succ },	
234	{ apply succ_le_succ,	$\forall a, b \in \mathbb{Z}, a+b \leq a + b $
 235	rw [← succ.inj e, ← add_assoc, add_comm],	
236	<pre>apply nat.le_add_right } },</pre>	
237	cases a; cases b with b b; simp [nat_abs, nat.succ_add];	
 238	try {refl}; [skip, rw add_comm a b]; apply this	
239	end	

My advice: Imagine your proof is being read by a skeptical friend who questions every statement you make For now: Err on the side of being too formal

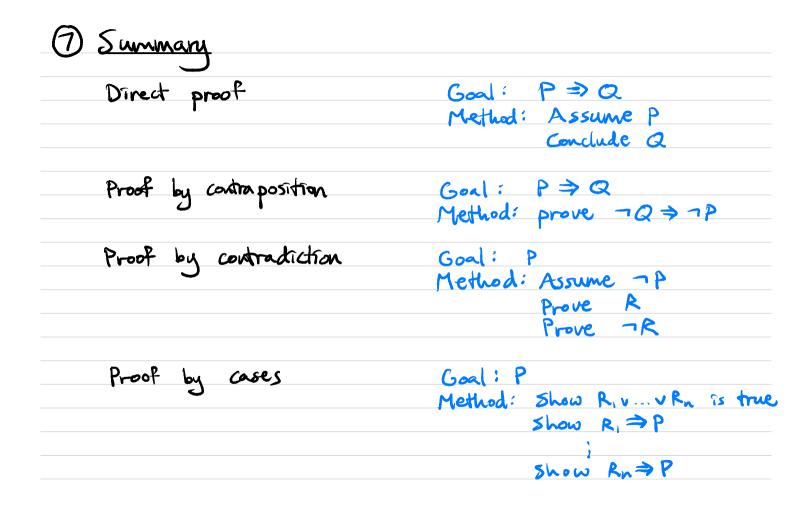
Proof by contraposition is especially useful if you are trying to prove something of the form $(\forall x P(x)) \Rightarrow (\forall y Q(y))$ $\begin{array}{rcl} \forall x P(x) \Rightarrow \forall y Q(y) &\equiv \neg (\forall y Q(y)) \Rightarrow \neg (\forall x P(x)) \\ &\equiv \exists y (\neg Q(y)) \Rightarrow \exists x (\neg P(x)) \end{array}$ Def A real number r is rational if there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $r = \frac{2}{5}$. Otherwise, r is irrational. Thus For every real number a, if a is irrational M rov then so is 3a. ∀a∈ R (a∉ Q ⇒ 3a∉Q) ∀piq∈Z a≠ ta Example e a real number. We will show that ronal then so is a. Assume 3a is rational. if Ra is national So there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $3a = \frac{p}{2}$. 3' gives us $a = \frac{p}{3q}$ vational. 5



Fact If
$$a \in \mathbb{Q}$$
 then there are $p, q \in \mathbb{Z}$ such that
 $q \neq 0$, $a = \frac{p}{2}$ and p and q share no common factors.
Imm JZ is invational.
Example proof suppose for contradiction JZ is rational. So by
the fact, there are $p, q \in \mathbb{Z}$ such that $q \neq 0$,
 p and q share no common factors and
 $JZ = \frac{p}{q}$.
Hence,
 $2 = (JZ)^2 = (\frac{p}{2})^2 = \frac{p^2}{q^2}$
Therefore p^2 is even, so by a thun from before, p is even
So by def, there is $k \in \mathbb{Z}$ such that $p = 2k$.
Hence
 $2 = \frac{p^2}{q^2} = p^2$.
Therefore p^2 is even, so by a thun from before, p is even
So by def, there is $k \in \mathbb{Z}$ such that $p = 2k$.
Hence
 $2 = \frac{p^2}{q^2} = (2k)^2 = 4k^2 = 2(2k^2)$
Dividing both sides by 2 gives $q^2 = 2k^2$, by the same
reasoning as before, q is even. This contradicts the fact
that p and q share no common factors.

Sometimes proof by cases is really cool, other times...
Fact For every natural number n, there is a natural
number K such that one of the following holds:

$$n=3k$$
 or $n=3k+1$ or $n=3k+2$
Thim For all $n \in N$, $3 \mid (n^3-n)$ went week, we'll see
another way to do this
proof Let n be a natural number and let K be
as in the fact above.
Case 1: $n = 3k$
 $n^3-n = (3k)^3 - 3k = 27k^3 - 3k = 3(9k^3-k)$
Case 2: $n = 3k+1$
 $n^3-n = (3k+1)^3 - (3k+1) = 27k^3 + 27k^2 + 9k+1 - 3k-1$
 $= 3(9k^3 + 9k^2 + 2k)$
Case 3: $n = 3k+2$
 $n^3-n = (3k+2)^3 - (3k+2) = 27k^3 + 54k^2 + 36k + 8 - 3k-2$
 $= 27k^3 + 54k^2 + 33k + 6 = 3(9k^3 + 18k^2 + 11k+2)$



(8) Other comments Today I wrote full proofs Usually: proof sketches < proofs you write on homework should be more complete than proofs in lecture/discussion Problem solving: Mink creatively, take leaps of faith, experiment, etc. Proof writing: every step must be justified and follow logically from previous steps A common pattern D Think about problem Come up with solution Try to write proof (4) Realize solution is wrong

9) Some tips When you are trying to prove something, ask yourself: What do I have/know? Definitions give you things! Look for the existential quantifiers! What an I trying to build/prove/etc? What conclusion are you working towards? Look for the existential quantifiers! What proofs have I seen before which do something similar to what I am trying to do here? Are those ideas helpful here?

Challenge question Can you find a propositional formula using only $P, Q, and \Lambda$ which is logically equivalent to $P \Rightarrow Q$? If not, can you prove it? what about logically equivalent to PAQ using only P, Q, and =>?