Proof by cases:

[there are two non-rational numbers x, y such that x^y is rational.

Idea - $(\sqrt{2})^2 = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = 2$

($\sqrt{2}$ to the $\sqrt{2}$ = x; x to the $\sqrt{2}$ = y)

non-rational $x = (\sqrt{2})^{\sqrt{2}}$

non-rational $y = \sqrt{2}$

s.t. $x^y = 2$ rational

Cases:

1) $x = (\sqrt{2})^{\sqrt{2}}$, $y = \sqrt{2}$

x is not rational

$\rightarrow x^y = 2$ is rational

can be rational or irrational ← 2) $(\sqrt{2})^{\sqrt{2}}$ is rational

$x = \sqrt{2}$, $y = \sqrt{2}$

x^y = rational

exam 1

07/11 ☆ Proof Methods:

Existence Proof ($\exists x P(x)$) by construction

ex) Given any $n \in \mathbb{N}$

$\exists\, m > n$, $n \in \mathbb{N}$ s.t. m is prime

Definition

$n \in \mathbb{N}$ is prime $\leftrightarrow$ n is divisible only by n and 1 → remainder $= 0$

Proof (by construction)

Let $n \in \mathbb{N}$

Let $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 5$, $p_5 = 7 \cdots p_r = n$ be the r prime numbers $\leq n$

(ex) $n = 7$; $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 5$, $p_5 = 7$)

Let $P = p_1 p_2 p_3 p_4 \cdots p_5 + 1$

if P is divided by p_k $\quad 1 \leq k \leq r$

(ex $P = 1 \cdot 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ → $2\overline{)211}$ ① $3\overline{)211}$ ① $5\overline{)211}$ ⊕ $7\overline{)211}$ ⊕

→ the remainder is 1

→ P is not divisible by $p_1, p_2, p_3 \cdots p_r = n$

2 parts

very Important!

Cases

1) P is divisible only by itself and 1 → P is prime and $P > n$

2) S divides P but $S \neq P_2, P_3, P_4 \cdots P_r$ (S: smallest prime number)

→ $S > n$

→ S is prime ∎

ex) Is 211 prime?

211/2 ··· no

211/3 ··· no

211/4 ··· no

211/5 ··· no

211/6 ··· no

⋮

~~211/10~~

211/14 ··· no

Only have to go up till 14, $14 \leq \sqrt{211}$

$ab = n$

→ $a \leq \sqrt{n}$ v $b \sqrt{n}$

211 is prime

211 77

Corollary:

The number of prime numbers is infinite.

2) Proof of uniqueness: ∃ exactly one x P(x)

a) ∃ x P(x)

b) Assume $X_1 P(x_1) \wedge X_2 P(X_2) \rightarrow X_1 = X_2$

ex) Show that there is a unique r such that $ar + b = 0$ where $a \neq 0$.

① prove that r exists

a) $ar + b = 0 \rightarrow ar = -b$

$r = -\frac{b}{a}$ it exists because $a \neq 0$

b) Let r_1 and r_2 satisfy:

$ar_1 + b = 0$ and $ar_2 + b = 0$

→ $ar_1 + b = ar_2 + b$

→ $ar_1 = ar_2$ since $a \neq 0$

→ $r_1 = r_2$ (only one value exists)

∴ ∃ a unique r s.t. $ar + b = 0$ where $a \neq 0$

Example of an Incorrect proof

Assume that $a=b$

$\rightarrow a+b=2b$

$\rightarrow a+b-2a=2b-2a$

$\rightarrow b-a=2(b-a)$

$\rightarrow \boxed{1=2}$

$\frac{b-a}{b-a}=2$

$\frac{b-b}{b-b}=2$

$\boxed{\frac{0}{0}=2=\text{indef.}}$

3) Proof by induction

Properties of $\mathbb{N}$ (axioms)

1) $1 \in \mathbb{N}$

2) $\forall n \in \mathbb{N}\ (S(n) \in \mathbb{N})$

$\neg\exists = \nexists$ (not exist)

3) $\nexists\, n \in \mathbb{N}\ (S(n)=1)$

$\forall n,m\ (S(n)=S(m))$

$n=m$

Successor function

$S(n)$ next element

$S(n)=n+1$

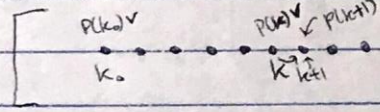
→ Induction axiom

ex) When we want to prove $\forall n \in \mathbb{N}\, P(n)$,

we use proof by induction

Basis ① show that $P(k_0)$ is true for the first $k_0 \in \mathbb{N}$

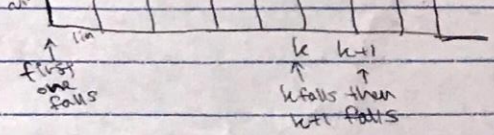
Inductive Hypothesis ② Assume $P(k)$ is true for a fixed $k \in \mathbb{N}$ s.t. $k \geq k_0$.



Assume it's consistent

Inductive step ③ Show that $P(k+1)$ is true.

ie. just like a domino



assuming everything else is the same then out.

ex) Show that

$\forall n \geq 1 \left(\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \right)$

* Using proof of induction you just have proof 1, k, and k+1

if $n = 5$ then

$1+2+3+4+5 = \frac{5(5+1)}{2}$

$15 = 15$ ✓

Proof of induction

1) Basis: $k_0 = 1$

$\rightarrow 1 = \frac{1(1+1)}{2}$

$1 = 1$ ✓

if this is not included then there's no diff. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

I.H. 2) Let k be a fixed number ($k \in \mathbb{N}$) $k \geq 1$

assume that

$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

I.S. 3) We want to show that

$\sum_{i=1}^{k+1} i = \boxed{\frac{(k+1)(k+2)}{2}}$

* Must use Inductive hyp. at some point

$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$

$= \underbrace{1+2+3+\cdots+k}+(k+1)$

using I.H. $= \frac{k(k+1)}{2} + (k+1)$

$= \frac{k(k+1) + 2(k+1)}{2}$

$= \boxed{\frac{(k+1)(k+2)}{2}}$ □ Proved

LECTURE 8

Examples

- There exist two irrational numbers x and y such that x^y is rational.
- Show that there is a unique r such that $ar + b = 0$ where $a \neq 0$
- Show that given two rational numbers there is always a rational number between them
- Given any positive integer r there is a prime number $p > r$

5.1 Proof by induction

Proofs by induction are used to show that properties linked somehow to the set of natural numbers are true. The idea is that we have a property $P(i)$ that depends on some natural number i, and we want to show that $P(i)$ is true for all possible integers n such that $n \geq b$, where b is a base value.

An example of a property like this is given in the following theorem.

Theorem 5.1 *For any integer n such that $n \geq 1$ it is always true that*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

This means that property $P(i)$ is true when the left and right hand sides of the equation are equal. We can show that $P(1)$ is true by expanding the left hand side and the right hand side of the equation.

$$\begin{aligned} \sum_{i=1}^{1} i &= \frac{1(1+1)}{2} \\ 1 &= \frac{1(2)}{2} \\ 1 &= 1 \end{aligned}$$

Therefore, we say that the property $P(n)$ is true for $n = 1$. Is the property true for $n = 4$, i.e. Is $P(4)$ true?. We can compute it to convince ourselves that it is indeed true.

$$\begin{aligned} \sum_{i=1}^{4} i &= \frac{4(4+1)}{2} \\ 1+2+3+4 &= \frac{4(5)}{2} \\ 10 &= 10 \end{aligned}$$

So far we know that $P(1)$ and $P(4)$ are true, but we don't know anything about $P(200)$. We would like to show that $P(n)$ is true for all integers $n \geq 1$, but this would require us to write an infinite number of proofs, one for each n.

Fortunately there is a way to prove that all the properties (an infinite number of them) are true, in three easy steps:

1. **Basis.**
   The first step is to show that $P(n)$ is true for the base value $n = b$.
2. **Inductive Hypothesis.**
   Then we must assume that the property $P(n)$ is true for a fixed value $n = k$ (we assume that $k \geq b$ is a fixed integer.
3. **Inductive Step.**
   Finally, we must use the *Inductive Hypothesis* to show that $P(n)$ is true for $n = k + 1$ (k is the fixed integer from the *Inductive Hypothesis*).

The intuitive idea is that if we can prove that the first element satisfies a given property, and assuming that one element satisfies it, we can show that the next one satisfies it too, then all elements must satisfy the property.

When writing proofs by induction it is important to:

- Indicate the variable that will be used in the proof. If the problem is simple enough, usually it only has one variable and it is clear what variable is being used. However, for problems involving several variables, it is not so obvious which one is the one that will be used in the proof.
- Explicitly label each one of the three steps.
- The Inductive Hypothesis must state that the assumption is only for a fixed k, otherwise, it appears as if we are assuming what we want to prove.
- In the *inductive step*, the *inductive hypothesis* must be used. If it appears as if you are not using the *inductive hypothesis*, it is very likely that you proof is wrong.

Examples

Prove by Induction each one of the following theorems:

1. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
2. The sum of the first n odd numbers is a perfect square
3. $\sum_{i=0}^{n} = 2^{n+1} - 1$
4. Geometric progression:

$$\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r-1}$$

when $r \neq 1$

5. $2^n < n!$
6. $n^3 - n$ is divisible by 3

EXAMPLE. Here is the first example in detail. The other examples will be given in class.

PROOF. (by induction on n)

1. **Basis.**
   If $n = 1$ we have that

$$\begin{aligned} \sum_{i=1}^{1} i &= \frac{1(1+1)}{2} \\ 1 &= \frac{1(2)}{2} \\ 1 &= 1 \end{aligned}$$

2. **Inductive Hypothesis.**
   Assume that for a fixed integer $k \geq 1$

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

3. **Inductive Step.**
   We need to show that

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

We will work on both sides of the equation independently in order to show that they are equal. First the left hand side:

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

Using the inductive hypothesis we get

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + (k+1)$$

using 2 as common denominator

$$\sum_{i=1}^{k+1} i = \frac{k(k+1) + 2(k+1)}{2}$$

now we factor $(k+1)$

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

So from the left hand side of the original equation we were able to obtain the right hand side. Therefore they are equal and the theorem is true.

□

There is a stronger version of induction that is used in more difficult cases. In this version, instead of assuming that the property $P(n)$ is true for $n = k$, for a fixed $k \geq b$, it is assumed that the property $P(n)$ is true for all $n \leq k$ for a fixed $k \geq b$. We might need to use this stronger version in our study of Discrete Mathematics.