# Lecture 33: Group Theory and linear algebra 21.10.2011

## Proof machine

First important point:

You cannot prove anything without having the definitions clearly stated.

Example Show that $-(-5)=5$ in the integers

This problem is impossible without knowing, exactly, the definition of $-x$.

## Types of proofs:

1. To show: If __A__ then __B__

   Assume __A__

   To show: __B__.

2. To show: There exists $x$ such that __C__

   Let $x =$ _____

   To show: __C__.

3. To show: $x$ such that __C__ is unique

   Assume $x$ satisfies __C__

   Assume $y$ satisfies __C__

   To show: $x=y$

## 4 Proofs by induction

To show: If $n \in \mathbb{Z}_{>0}$ then $\underline{\quad B \quad}$

<u>Base Case: $n=1$.</u>

Assume $n=1$.

To show: $\underline{\quad B \quad}$

⋮

<u>Base Case: $n=2$</u>

Assume $n=2$

To show: $\underline{B}$

⋮

<u>Base Case: $n=3$</u>

Assume $n=3$

To show: $\underline{B}$

⋮

Do enough base cases so that the pattern is clear.

<u>Induction step</u>

Assume that if $k \in \mathbb{Z}_{>0}$ and $k < n$ then $\underline{B}$.

To show: $\underline{\quad B \quad}$

⋮

This proof should be exactly the same as your last base case (say you did base cases to $n=5$) except with $n$ replacing 5.

5 Proofs by contradiction

To show: If A and B and C then D

Assume A

Assume B

Assume C

Proof by contradiction.

Assume not D

Then

⋮ Proceed until you derive a contradiction to something that was assumed.

Then not B

This is a contradiction to B

So if A and B and C then D.

Proof

A proof is the explanation of why something is true.

Proof machine is a way of formulation this explanation in an organised way which conforms to the conventions of logical sequencing.

A remark on the definition of <u>isometry</u>

<u>Definition 2.4.6</u> p. 56 of Groves-Hodgson:

Let $f$ be a linear transformation on an inner product space $V$.

$f$ is an <u>isometry</u> if $f^*f = id_V$.

<u>§3.8.4</u> p. 118 of Groves-Hodgson

An <u>isometry</u> of $\mathbb{E}^n$ is a function $f: \mathbb{R}^n \to \mathbb{R}^n$ such that if $x, y \in \mathbb{R}^n$ then

$$d(x,y) = d(f(x), f(y))$$

Explain why these two uses of the term "isometry" are not inconsistent.

Assume $f: \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation.

To show: (a) If $f$ satisfies $f^*f = id$

then $f$ satisfies

if $x, y \in \mathbb{R}^n$ then $d(x,y) = d(fx, fy)$

(b) If $f$ satisfies

if $x, y \in \mathbb{R}^n$ then $d(x,y) = d(fx, fy)$

then $f$ satisfies $f^*f = id$.