Lecture 25 : Groups (math from Axioms)

<u>defn</u> A <u>group</u> is a set G equipped with a binary operation "$\cdot$" and a special element $1 \in G$ satisfying the following axioms:

(i) $\forall\, g, h, k \in G, \quad (g \cdot h) \cdot k = g \cdot (h \cdot k)$ (associativity)

(ii) $\forall\, g \in G, \quad g \cdot 1 = g = 1 \cdot g$ (identity element)

(iii) $\forall\, g \in G, \ \exists\, g^{-1} \in G$ s.t. $g \cdot g^{-1} = 1 = g^{-1} \cdot g$. (existence of inverses)

<u>Prop D.1</u> Given $g \in G$, g^{-1} in (iii) is <u>unique</u>.

Pf.

Suppose $h_1, h_2 \in G$ satisfy $g \cdot h_1 = 1 = g \cdot h_2$.

Then $g^{-1} \cdot g \cdot h_1 = g^{-1} \cdot g \cdot h_2$, so $1 \cdot h_1 = 1 \cdot h_2$, so $h_1 = h_2$. ∎

<u>Prop D.1 (2nd part)</u> The $1 \in G$ is the unique element in G such that (ii) holds.

Pf.

Suppose we have $e \in G$ s.t. $\forall g$, $g \cdot e = g$.

Then $g^{-1} g \cdot e = g^{-1} \cdot g = 1$ so $e = 1$. ∎