Groups in HOL

- Oversimple HOL definition of a group

  $\vdash \mathsf{Group}(\bullet{:}\alpha{\to}\alpha{\to}\alpha)\ \sim\ \imath\ =$
  $(\forall \mathtt{x}\ \mathtt{y}\ \mathtt{z}.\ \mathtt{x} \bullet (\mathtt{y} \bullet \mathtt{z}) = (\mathtt{x} \bullet \mathtt{y}) \bullet \mathtt{z})\ \wedge$
  $(\forall \mathtt{x}.\ \mathtt{x} \bullet \imath = \mathtt{x})\ \wedge$
  $(\forall \mathtt{x}.\ \mathtt{x} \bullet \sim\mathtt{x} = \imath)$

- Easy to prove:

  $\vdash \mathsf{Group}\ \bullet\ \imath\ \sim\ \Rightarrow (\sim\mathtt{x} \bullet \mathtt{x} = \imath)$

  $\vdash \mathsf{Group}\ \bullet\ \imath\ \sim\ \Rightarrow (\imath \bullet \mathtt{x} = \mathtt{x})$

- Theorems about subgroups hard to express