Existence of a Unique Inverse Element
Homework On Proof Systems

Néstor Cataño C.
ncatano@puj.edu.co

You shall carry out the formal proof of a theorem in *group theory*. A group is a structure $(G, e, *)$, where $e \in G$ is called the *module* of the group, and $*$ is a binary relation over G. In the following, x, y, and z will be elements in G. A group satisfies the following three axioms :

module	$\forall x.\ x * e \equiv x \ \wedge\ e * x \equiv x$
inverse	$\forall x.\ \exists y.\ x * y \equiv e \ \wedge\ y * x \equiv e$
associativity	$\forall x.\ \forall y.\ \forall z.\ (x * y) * z \equiv x * (y * z)$

where $\equiv$ is an *equivalence relation* over G, *i.e.*, a relation over G satisfying the following three axioms :

reflexivity	$\forall x.\ x \equiv x$
symmetry	$\forall x.\ \forall y.\ x \equiv y \rightarrow y \equiv x$
transitivity	$\forall x.\ \forall y.\ \forall z.\ (x \equiv y \ \wedge\ y \equiv z) \rightarrow x \equiv z$

Additionally, suppose that a **uniformity** property over G exists.

uniformity	$\forall x.\ \forall y.\ \forall z.\ x \equiv y \rightarrow (x * z \equiv y * z \ \wedge\ z * x \equiv z * y)$

You shall carry out the formal proof of the theorem "any element in G has a unique *inverse* element". An element x has an inverse y if both $x * y \equiv e$ and $y * x \equiv e$. The proof of this theorem as it appears in texts of mathematics is given below. To carry out the proof, for any element in the group, the existence of two inverse elements is supposed, which are then proved to be equals. Let us assume that x has two inverse elements b and c. It follows that :

$x * b \equiv e \ \wedge\ x * c \equiv e$	(definition of inverse element)
$x * b \equiv x * c$	(cause $x * b$ and $x * c$ are both equals to e)
$b * x * b \equiv b * x * c$	(multiplying on the left by b)
$e * b \equiv e * c$	(because $b * x \equiv e$)
$b \equiv c$	(by **module**)

You shall carry out the *formal proof* of the theorem presented above, which is formally stated as "$\forall x.\ \forall b.\ \forall c.\ (x * b \equiv e \ \wedge\ b * x \equiv e \ \wedge\ x * c \equiv e \ \wedge\ c * x \equiv e) \rightarrow b \equiv c$". You are allowed to use the proof system introduced in class, and any of the deduction rules `skolemize`, `instantiate`, `flatten`, `replace`, `split`, etc.