Computing and Software 734
Formalized Mathematics

William M. Farmer
McMaster University, Winter 2014

Exercise 4

20 pts.
Due 4 March 2014

Assigned: 7 February 2014
Revised: 7 February 2014

Using your chosen proof assistant, create a theory of an abstract group called something like Group by extending your theory Monoid. Add to Monoid a new constant inv of type $\mathsf{mon} \rightarrow \mathsf{mon}$ and axioms that say $\mathsf{inv}(x)$ is a left and right inverse of x with respect to mul. Prove the following lemmas:

1. $\forall\, x, y : \mathsf{mon}\ .\ \mathsf{inv}(x)\ \mathsf{mul}\ (x\ \mathsf{mul}\ y) = y$.
2. $\forall\, x, y : \mathsf{mon}\ .\ x\ \mathsf{mul}\ (\mathsf{inv}(x)\ \mathsf{mul}\ y) = y$.
3. $\mathsf{inv}(\mathsf{e}) = \mathsf{e}$.
4. $\forall\, x : \mathsf{mon}\ .\ \mathsf{inv}(\mathsf{inv}(x)) = x$.
5. $\forall\, x, y : \mathsf{mon}\ .\ \mathsf{inv}(g\ \mathsf{mul}\ h) = \mathsf{inv}(h)\ \mathsf{mul}\ \mathsf{inv}(g)$.
6. $\forall\, x, y, z : \mathsf{mon}\ .\ x\ \mathsf{mul}\ y = x\ \mathsf{mul}\ z \Leftrightarrow y = z$.
7. $\forall\, x, y, z : \mathsf{mon}\ .\ y\ \mathsf{mul}\ x = z\ \mathsf{mul}\ x \Leftrightarrow y = z$.

Send the instructor the files you produced with comments and instructions on how they can be loaded and checked.