CSE607
Theories with Equality and Algebra Exam
Exam#3 April 1, 2002

This is an open-book and open-notes examination. Do all problems in 80 minutes. Make sure you justify your steps using the formal inference rules to earn full credit. (This includes rewriting rules—this will help you to avoid silly mistakes). *Left justify assumptions and indent goals* – it makes evaluating your proofs easier.

1. **(15 points) Relations and Orders**
   **(10 points for setting up the proof; 5 points for the proof)**

   Let R(x, y) be a relation that is
   - Transitive
   - Irreflexive

   Let S(x, y) be a relation that is
   - Transitive
   - Symmetric
   - Reflexive

   Let relation Q be defined as
   \[ \forall x, y. (Q(x, y) \equiv R(x, y) \lor S(x, y)) \]

   Prove there exists a case where Q(x, y) and Q(y, x) are both true.

2. **(10 points) Prove the following**

   A0. \( x = x \)
   A1. \( x \circ e = x \)
   A2. \( x \circ x^{-1} = e \)
   A3. \( (y \circ x) \circ z = y \circ (x \circ z) \)

   G1. \( \forall x, y, z. [(y \circ z = x \circ z) \Rightarrow (y = x)] \)

3. **(15 points) Prove the following**

   A1. Whoever cooperates with Deena will hire Cindy.
   A2. Jenny hires only for friends of Laura.
   A3. No one is a friend of Kelly and has Cindy as a friend.
   G1. If Laura is a friend of Kelly, Jenny will not cooperate with Deena.

   A. **(10 points of 15)** Use the following notation to translate the above statements into symbolic form:

   - C(x, y): x cooperates with y
   - H(x, y): x hires y
   - F(x, y): x is a friend of y
   - d: Deena, c: Cindy, j: Jenny, l: Laura, k: Kelly

   B. **(5 points of 15)** Proven the goal G1 given assumptions A1, A2, and A3. Make sure you justify each step in the tableau.
• **Bonus Problem (5 points)** Please prove G1 by using the following assumptions and the knowledge introduced in [Ferraiolo et al. 1999].

Please use the following notation:
- \( U(x) : x \) is a user
- \( R(x) : x \) is a role
- \( P(x) : x \) is a permission
- \( RM(r, u) : u \) is a member of role \( r \)
- \( Ea(i, j) : i \) and \( j \) are mutually exclusive roles

Role Membership Inheritance: 
\[
(\forall i, j : role)(\forall u : user).([(i \geq j) \land RM(i, u) \supset RM(j, u)]
\]

Static Separation of Duty: 
\[
(\forall u : user)(\forall i, j : role).[(RM(i, u) \land RM(j, u)) \supset \neg Ea(i, j)]
\]

A1. Harry is authorized for role 1.
A2. Role 1 contains role 2.
A3. Role 3 is mutually exclusive with role 2.

G1. Harry can not be authorized for role 3.

Use the following notation:
- \( H : \) Harry, \( r1: role 1, r2, role 2, r3: role 3 \)

Reference: