Rowan Lochrin
MATH3066
Homework 2
31/5/17

1. (a) $(\exists x)(F(x) \wedge (\forall y)G(x,y)) \vdash (\forall y)(\exists x)(F(x) \wedge G(x,y))$

1	(1)	$(\exists x)(F(x) \wedge (\forall y)G(x,y))$	A	
2	(2)	$F(a) \wedge (\forall y)G(a,y)$	A	
3	(2)	$F(a)$	2	$\wedge - E$
4	(2)	$(\forall y)G(b,y)$	2	$\wedge - E$
5	(2)	$G(a,b)$	4	$\forall - E$
6	(2)	$F(a) \wedge G(a,b)$	$3,5$	$\wedge - I$
7	(2)	$\exists x(F(x) \wedge G(x,b))$	6	$\exists - I$
8	(1)	$(\exists x)(F(x) \wedge G(x,b))$	$1,2,6$	$\exists - E$
9	(1)	$(\forall y)(\exists x)(F(x) \wedge G(x,y))$	8	$\forall - I$

(b) $(\forall a)((F(x) \vee G(x)) \Rightarrow H(x)) \vdash (\exists x) \sim F(x)$

1	(1)	$(\forall a)((F(x) \vee G(x)) \Rightarrow H(x))$	A	
2	(2)	$(\exists x) \sim H(x)$	A	
3	(3)	$\sim H(a)$	A	
4	(1)	$(F(a) \vee G(a)) \Rightarrow H(a)$	1	$\exists - E$
5	$(1,3)$	$\sim (F(a) \vee G(a))$	$3,4$	MT
6	(6)	$F(a)$	A	
7	(6)	$F(a) \vee G(a)$	6	$\vee - I$
8	$(1,3,6)$	$\sim (F(a) \vee G(a)) \wedge (F(a) \vee G(a))$	$5,7$	$\wedge - I$
9	$(1,3)$	$\sim F(a)$	$1,3,6,8$	AA
10	$(1,3)$	$(\exists x) \sim F(x)$	9	$\exists - I$
11	$(1,2)$	$(\exists x) \sim F(x)$	$2,3,10$	$\exists - E$

(c) $(\forall a)(\forall y)(H(y,y) \Rightarrow \sim H(y,y)) \vdash (\forall a) \sim H(x,x)$

1	(1)	$(\forall a)(\forall y)(H(y,y) \Rightarrow \sim H(y,y))$	A	
2	(1)	$(\forall y)(H(y,y) \Rightarrow \sim H(y,y)$	1	$\forall - E$
3	(1)	$H(a,a) \Rightarrow \sim H(a,a)$	2	$\forall - E$
4	(4)	$H(a,a)$	A	
5	$(1,4)$	$\sim H(a,a)$	$3,4$	MP
6	$(1,4)$	$H(a,a) \wedge \sim H(a,a)$	$5,6$	$\wedge - I$
8	(1)	$\sim H(a,a)$	$1,4,6$	AA
9	(1)	$(\forall a) \sim H(x,x)$	8	$\forall - I$

2. (a) i. The theorem that this is attempting to prove is correct however:

$$\sim \forall a \sim G(x) \vdash \sim\sim G(a)$$

is not a valid instance of universal instantiation because $\forall x$ does not appear in the front of the WFF.

ii. The problem here is in the existential generalization on line 9. The author seeks to replace the assumption of $G(a)$ with $(\exists x)G(x)$. This is not a valid instance of existential generalization as a appears in one of the assumptions for line 9 (line 2: $\sim G(a)$).

(b) Consider $U = \{a, b\}$ let:

$$F = \{a\}$$
$$G = \{b\}$$

We can see that $(\exists x)F(x) = T$ and $(\exists x)G(x) = T$, so the antecedent of or sequent is true. However $\sim G(a) \Rightarrow \sim F(a) = F$ so the consequent must be false.

3. (a) Note that in a model with only one element for any WFF involving letters a,b, a = b. Meaning:

$$W_1 \to (\exists x)H(x, x)$$
$$W_2 \to (\forall a)(H(x, x) \Rightarrow \sim H(x, x))$$

So if our model has only one element, a, by W_1 we know $H(a, a)$ but $H(a, a)$, implies $\sim H(a, a)$ by W_2 so we have a contradiction.

(b) If $a = (x_1, x_2) \in \mathcal{U} \times \mathcal{U}$ if $x \notin K$ then $x \in H$ by W_3 so $x \in H \cup K$. If $x \in H \cup K$ then $x \in \mathcal{U} \times \mathcal{U}$ by definition. So $\mathcal{U} \times \mathcal{U} = H \cup K$. H and K are disjoint as any member of K cannot be a member of H again by W_3.

(c) W_2 implies that no elements of the diagonal relation are in H (see part a).W_3 implies that every element not in H must be in K.

(d) $\mathcal{U}$ cannot have 0 elements by definition, it can't have 1 element by part a. Suppose $\mathcal{U}$ has 2 elements - a, b - than by W_1 without loss of generality $H(a, b)$, so by W_3, $\sim K(a, b)$. Meaning that by the second disjunct of W_4 either $H(b, a) \wedge H(a, a)$ or $H(b, b) \wedge H(b, y)$. However because we have $H(a, b)$ W_2 gives us $\sim H(b, a)$ so neither of these can be true, giving us a contradiction.

(e) Consider $U = \{a, b, c\}$:

$$H = \{(a, b), (b, c), (c, a)\}$$
$$K = (\mathcal{U} \times \mathcal{U}) \setminus H$$

This is a valid model. There must always be 3 elements of H when there are 3 elements in $\mathcal{U}$. W_1 tells us that there is at least one element of H. W_3 and W_4 tell us that if $\exists(a, b) \in H$ then there must also $\exists(b, c), (c, a) \in H$ so the number of elements in H must be a multiple for 3. If there were 6, or 9, elements in H then by W_2 there would have to be 12 or 18 elements in $\mathcal{U} \times \mathcal{U}$ which contradicts our assumption that there are 3 elements in $\mathcal{U}$, so there must be 3 elements in H.

4. (a) $x = \frac{2}{3}$ in $\mathbb{Z}_{13}$ where $3x = 2 \mod 13$ meaning:

$$x = 2 * 3^{-1} \mod 13 = 2 * 9 \mod 13 = 5$$

(b) $x = \frac{2}{3}$ in $\mathbb{Z}_{12}$

$$3x = 2 \mod 12$$

Because $gcd(3, 12) = 3 > 2$ this equation has no solution.

(c) $x = \frac{6}{9}$ in $\mathbb{Z}_{12}$

$$9x = 6 \mod 12 \to 3x = 2 \mod 4 \to x = 2 \mod 4$$

Meaning that 2, 6 and 10 all solve this equation.

(d) $x = \frac{6}{9}$ in $\mathbb{Z}_{16}$

$$x = 6 * 9^{-1} \mod 16 \rightarrow x = 6 * 9 \mod 16 \rightarrow x = 6 \mod 16$$

(a) Assume $p(x)$ is reducible then for some a, b:

$$x^2 + 1 = (x + a)(x + b) = x^2 + (a + b)x + ab$$

However there are no two elements $a, b \in \mathbb{Z}_3$ such that $a + b = 0$ and $ab = 1$.

(b) $x + 1$ is a primitive root as:

$$\{(x + 1)^n : n \in [1, 2...9]\} = R$$

That is to say $x + 1$ spans R x is not a primitive root as $x^5 = x$ so it does not span R.

(c) in R $(2x + 1)^2 = x$ and $(x + 2)^2 = x$ so these are both square roots of x.

(d) The only solutions of this equation are the square roots of x ($2x + 1$ and $x + 2$) as the equation can only be factored when $\alpha^2 = x$.

5. (a) Consider the homomorphism $\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$ defined by $\phi(P) = P(\sqrt{k}i)$. For all elements $(a+bi) \in \mathbb{C}$ There exists an element $(\frac{b}{\sqrt{k}}x+a) \in \mathbb{R}[x]$ such that $\phi(\frac{b}{\sqrt{k}}x+a) = a + bi$ so ϕ is onto meaning im$\phi = \mathbb{C}$. If $\phi(P) = 0$ then $\sqrt{k}i$ is a root of P so P must be divisible $x^2 + k$ meaning ker$\phi = (x^2 + k)R[x]$. So by the first isomorphism theory $\mathbb{R}[x]/(x^2 + k)\mathbb{R}[x] = \mathbb{C}$.
Consider the homomorphism $\phi : \mathbb{R}[x] \rightarrow \mathbb{R} \oplus \mathbb{R}$ defined by $\phi(P) = (P(\sqrt{k}), -P(\sqrt{k}))$. This homomorphism is onto and its kernel $(x^2 - k)\mathbb{R}[x]$. So by the first isomorphism theory $\mathbb{R}[x]/(x^2 - k)R[x] = \mathbb{R} \oplus \mathbb{R}$.

(b) Because $\mathbb{C}$ is not isomorphic to $\mathbb{R} \oplus \mathbb{R}$, by part a S_1 cannot be isomorphic to S_2. Assume S_3 is isomorphic to S_2 by the first isomorphism theory there exists an isomorphism ϕ such that ker$\phi = (x^2)\mathbb{R}[x]$ and in$\phi = S_2$. Define ϕ' to be $\phi'(x) = \phi^{-1}(x) + 1$ meaning ker$\phi' = (x^2)\mathbb{R}[x]$ and in$\phi' = S_1$. So again by the first isomorphism theory S_1 must also be isomorphic to S_3. Because 3_2 and S_3 are not isomorphic themselves S_3 cannot be isomorphic to both of them so S_3 must not be isomorphic to S_2. S_3 cannot be isomorphic to S_1 by similar reasoning.