MATH3066 A2 500468777

Question 1

$$(\exists x)(G(x) \implies (H(x) \wedge K(x)), (\forall x) \sim K(x) \vdash (\exists x) \sim G(x)$$

Assumptions	#	Formula	Rule
	1	(∃x)(G(x) ⇒ (H(x)∧ K(x))	A
	2	(∀x) ~ K(x)	A
	3	G(a) ⇒ (H(a)∧ K(a))	A
2	4	~ k(a)	2 ∀E
	5	G(a)	A
3, 5	6	H(a)∧ K(a)	5, 3 MP
3, 5	7	k(a)	6 ∧E
2, 3, 5	8	k(a)∧ ~ k(a)	7, 4 ∧I
2, 3	9	~ G(a)	8 RAA
2, 3	10	(∃x)~ G(x)	9 ∃I
1, 2	11	(∃x)~ G(x)	1, 3, 10 ∃E

Question 2

Part a

In line 7, existential elimination is used to dispel the assumption of line 3 and replace it with the pooled assumptions of line two. However, existential elimination requires the constant value to not appear in the WFF that has been deduced. $G(a) \wedge H(a)$ is the WFF referenced in line 6 and clearly still contains the constant symbol a that is being replaced. Hence this line is logically flawed.

Part b

Let:

- U = $\mathbb{N}$ = {1, 2, 3, 4 ...}
- G = $\{2x : x \in \mathbb{N}\}$ = set of even numbers
- H = $\{x : x > 0\}$ = set of numbers greater than 0

Then:

- $G(2) = T \implies (\exists x)G(x)$

- $\forall x \in N : x > 0 \implies (\forall x) H(x)$

Thus $(\exists x) G(x) \land (\forall x) H(x)$

But for x = 3:

- $H(3) = F \implies (G(x) \land H(3)) = F$
- $\implies (\exists x) \sim (G(x) \land H(x))$
- $\implies \sim (\forall x)(G(x) \land H(x))$

Thus

$$(\exists x) G(x) \land (\forall x) H(x) \nvdash (\forall x)(G(x) \land H(x))$$

By soundness metatheorem:

$$(\exists x) G(x) \land (\forall x) H(x) \nvdash (\forall x)(G(x) \land H(x))$$

Part c

$$(\forall x)(G(x) \land H(x)) \vdash ((\exists x) G(x)) \land ((\forall y) H(y))$$

Assumptions	#	Formula	Rule
	1	(∀x) (G(x) ∧ H(x))	A
1	2	G(a) ∧ H(a)	1 ∀E
1	3	G(a)	2 ∧E
1	4	(∃x)G(x)	3 ∃I
1	5	H(a)	2 ∧E
1	6	(∀y) H(y)	5 ∀I
1	7	((∃x)G(x))∧ ((∃y) H(y))	4, 6 ∧I

Question 3

Considering W_1:

Assumptions	#	Formula	Rule
	1	(∀x)(E(x,x)∧(G(x)∨ H(x)))	A
1	2	(E(a,a)∧(G(a)∨ H(a)))	1 ∀E
1	3	E(a,a)	2 ∧E
1	4	(∀x)E(x,x)	3 ∀I
1	5	G(a)∨ H(a)	2 ∧E
1	6	(∀x) (G(x) ∨ H(x))	5 ∀I

From lines 4 and 6 we have:

1. $W_1 \vdash (\forall x)E(x,x)$
2. $W_1 \vdash (\forall x)(G(x) \vee H(x))$

Consider $W_3 \wedge W_4$:

$$(\exists x)(\exists y)(\sim G(x) \wedge \sim G(y) \wedge \sim E(x,y)) \ \wedge \ (\exists x)(\exists y)(\sim H(x) \wedge \sim H(y) \wedge \sim E(x,y))$$

Without loss of generality, assume a, b, c and d to be a satisfying assignment of the variables, yielding:

$$(\sim G(a) \wedge \sim G(b) \wedge \sim E(a,b)) \ \wedge \ (\sim H(c) \wedge \sim H(d) \wedge \sim E(c,d))$$
$$= \sim G(a) \wedge \sim G(b) \wedge \sim E(a,b) \ \wedge \ \sim H(c) \wedge \sim H(d) \wedge \sim E(c,d)$$

Now, considering $W_1 \wedge W_3 \wedge W_4$:

- $a = b \implies \sim E(a,a)$ false by (1)
- $a = c \implies \sim G(a) \wedge \sim H(a)$ false by (2)
- $a = d \implies \sim G(a) \wedge \sim H(a)$ false by (2)
- $b = c \implies \sim G(b) \wedge \sim H(b)$ false by (2)
- $b = d \implies \sim G(b) \wedge \sim H(b)$ false by (2)
- $c = d \implies \sim E(c,c)$ false by (1)
  Thus $a \neq b \neq c \neq d \implies$ there are at least 4 elements in the model

Finally, considering $W_2 = (\exists x)(G(x) \wedge H(x))$:
$W_1 \wedge W_2 \wedge W_3 \wedge W_4$ implies there exists an element, e satisfying both G(e) and H(e).
- $e = a \implies \sim G(e)$
- $e = b \implies \sim G(e)$
- $e = c \implies \sim H(e)$
- $e = d \implies \sim H(e)$

Thus e cannot be any a, b, c or d.
Thus, any model satisfying $W_1 \wedge W_2 \wedge W_3 \wedge W_4$ must contain at least 5 distinct elements.

Consider the following model with:

- U = $\mathbb{Z}_5$ ={0, 1, 2, 3, 4}
- E = {$(x,y) \subseteq$ U^2 : $x = y$} = {pairs of numbers that are equal}
- G = {$x \in$ U : $x > 1$} = {2, 3, 4}
- H = {$x \in$ U : $x < 3$} = {0, 1, 2}

Then:

1. Every number is equal to itself and G $\cup$ H = U
   $\implies (\forall x)(E(x,x) \wedge (G(x) \vee H(x))) \implies W_1 = T$
2. G $\cap$ H = {2} $\implies$ G(2) $\wedge$ H(2) $\implies (\exists x)(G(x) \wedge H(x)) \implies W_2 = T$

3. $(\sim G(0) \wedge \sim G(1) \wedge \sim E(0,1)) \implies (\exists x)(\exists y)(\sim G(x) \wedge \sim G(y) \wedge \sim E(x,y)) \implies W_3 = T$
4. $(\sim H(3) \wedge \sim H(4) \wedge \sim E(3,4)) \implies (\exists x)(\exists y)(\sim H(x) \wedge \sim H(y) \wedge \sim E(x,y)) \implies W_4 = T$

Thus this model satisfies $W_1 \wedge W_2 \wedge W_3 \wedge W_4$ and contains 5 elements

Question 4

For $\bar{\beta} = 2 - i + j - k$:

$$\beta\bar{\beta} = \bar{\beta}\beta = 2^2 + 1^2 + 1^2 + 1^2 = 7$$

Thus:

$$\begin{aligned}
\beta\gamma &= 3j - 4k \\
\implies \bar{\beta}\beta\gamma &= \bar{\beta}(3j - 4k) \\
\implies 7\gamma &= (2 - i + j - k)(3j - 4k) \\
\implies \gamma &= \frac{1}{7}(6j - 3ij + 3j^2 - 3kj - 8k + 4ik - 4jk + 4k^2) \\
&= \frac{1}{7}(6j - 3k - 3 + 3i - 8k - 4j - 4i - 4) \\
&= \frac{1}{7}(-7 - i + 2j - 11k)
\end{aligned}$$

$$\begin{aligned}
\delta\beta &= 3j - 4k \\
\implies \delta\beta\bar{\beta} &= (3j - 4k)\bar{\beta} \\
\implies 7\gamma &= (3j - 4k)(2 - i + j - k) \\
\implies \gamma &= \frac{1}{7}(6j - 3ji + 3j^2 - 3jk - 8k + 4ki - 4kj + 4k^2) \\
&= \frac{1}{7}(6j + 3k - 3 - 3i - 8k + 4j + 4i - 4) \\
&= \frac{1}{7}(-7 + i + 10j - 5k)
\end{aligned}$$

Question 5

Part a

	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

From the multiplication table above it can be seen that each element is contained only once for each column and row. Thus, each element has an inverse element that, when multiplied, yields the identity element. Thus, as R is a commutative ring and each element has an inverse, R is a field.

Part b

$f(\alpha) = \alpha^3 + \alpha x + x^2 + 1 = 0$
$f(1) = 0 \implies f(\alpha) = (\alpha + 1)(\alpha^2 + \alpha k(x) + x^2 + 1) = \alpha^3 + \alpha^2(k(x) + 1) + \alpha(k(x) + x^2 + 1) + x^2 +$

Equating coefficients of x^2:
$0 = k(x) + 1$
$\implies k(x) = 1$

Now:
$f(\alpha) = (\alpha + 1)(\alpha^2 + \alpha + x^2 + 1)$
$\implies \alpha^2 + \alpha + x^2 + 1 = 0$
$\implies \alpha^2 + \alpha = x^2 + 1$

By inspection of the table:
$\alpha = x^2 + x$
$\implies \alpha^2 + \alpha = (x^2 + x)^2 + x^2 + x)$
$= x + 1 + x^2 + x$
$= x^2 + 1$
$= RHS$
$\alpha = x^2 + x + 1$
$\implies \alpha^2 + \alpha = (x^2 + x + 1)^2 + x^2 + x + 1)$
$= x + x^2 + x + 1$
$= x^2 + 1$
$= RHS$

Thus:
$f(\alpha) = (\alpha + 1)(\alpha + x^2 + 1)(\alpha + x^2 + x)$

And
$f(\alpha) = 0 \implies \alpha = 1, \alpha = x^2 + x + 1, \alpha = x^2 + x$

Question 6

Part a

$(1 - e)$ idempotent if $(1 - e)^2 = 1 - e$

$$\begin{aligned}(1 - e)^2 &= 1 - 2e + e^2 \\ &= 1 - 2e + e^2 \text{ (if e idempotent)} \\ &= 1 - e\end{aligned}$$

Thus $e\ idempotent \implies (1-e)\ idempotent$

Part b

Assume $e^2 = e$ in R
$eR = \{er | r \in R\}$
Define $\alpha, \beta \in eR$ where $\alpha = ea$ and $\beta = eb$ for $a, b \in R$

Then:

$$\begin{aligned}\alpha + \beta &= ea + eb \\ &= e(a+b) \text{ (by distributivity of } + \text{ and x in R)} \\ &\in eR \text{ as R closed under addition} \\ &\implies eR \text{ closed under addition}\end{aligned}$$

$$\begin{aligned}\alpha\beta &= (ea)(eb) \\ &= e^2(ab) \text{ (as x commutative in R)} \\ &= e(ab) \\ &\in eR \text{ as R closed under multiplication} \\ &\implies eR \text{ closed under multiplication}\end{aligned}$$

$$\begin{aligned}-\alpha &= -ea \\ &= e(-a) \text{ (by commutivity of x in R)} \\ &\in eR \text{ as R closed under negation} \\ &\implies eR \text{ closed under negation}\end{aligned}$$

$$\begin{aligned}\alpha\beta &= (ea)(eb) \\ &= (eb)(ea) \text{ (as x commutative in R)} \\ &= \beta\alpha \\ &\implies \text{x commutative in eR}\end{aligned}$$

Finally, $1 \in R \implies e \in eR$ as $e = 1e$ and as $e^2 = e$:

$$\begin{aligned}e\alpha &= e(ea) \\ &= e^2a \text{ as x assosciative in R} \\ &= ea \\ &= \alpha \\ &= \alpha e \text{ as mulitplication commutative} \\ &\implies \text{eR has multiplicative identity, e}\end{aligned}$$

Thus, eR is a commutative subring with identity.

Part c

RTP: $R \cong eR \oplus (1-e)R$
Define

$$\begin{aligned}\varphi : R &\to eR \oplus (1-e)R \\ a &\mapsto (ae, (1-e)a)\end{aligned}$$

Then, for $a, b \in R$:

$$\begin{aligned} a\varphi + b\varphi &= (ea, (1-e)a) + (eb, (1-e)b) \\ &= (ea + eb, (1-e)a + (1-e)b) \\ &= (e(a+b), (1-e)(a+b)) \\ &= (a+b)\varphi \\ &\implies \varphi \text{ preserves addition} \end{aligned}$$

$$\begin{aligned} (a\varphi)(b\varphi) &= (ea, (1-e)a)(eb, (1-e)b) \\ &= ((ea)(eb), ((1-e)a)((1-e)b)) \\ &= (e^2(ab), (1-e)^2(ab)) \\ &= (e(ab), (1-e)(ab)) \text{ as e and 1-e idempotent} \\ &= (ab)\varphi \\ &\implies \varphi \text{ preserves multiplication} \end{aligned}$$

Thus φ is a homomorphism as it preserves the ring operations

Now, define:

$$\begin{aligned} \varphi^{-1} : eR \oplus (1-e)R &\to R \\ (et, (1-e)s) &\mapsto et + (1-e)s \end{aligned}$$

Then:

$$\begin{aligned} ((et, (1-e)s)\varphi^{-1})\varphi &= (et + (1-e)s)\varphi \\ &= (e(et + (1-e)s), (1-e)(et + (1-e)s)) \\ &= (e^2t + (e-e^2)s, (e-e^2)t + (1-e)s) \\ &= (et + (e-e)s, (e-e)t + (1-e)s) \\ &= (et, (1-e)s) \end{aligned}$$

Thus φ has a well defined inverse and thus is surjective.

Now if $a\varphi = b\varphi$:

$$\begin{aligned} a\varphi &= b\varphi \\ \implies (ea, (1-e)a) &= (eb, (1-e)b) \\ \implies ea = eb \; and \; (1-e)a &= (1-e)b \\ \implies a - ea &= b - eb \\ \implies a - eb &= b - eb \text{ (as ea = eb)} \\ \implies a &= b \end{aligned}$$

Thus φ is injective and hence bijective.
Thus there exists a bijection $\varphi : R \to eR \oplus (1-e)R \implies R \cong eR \oplus (1-e)R$

Question 7

Part a

0, 1, 6, 10, 15, 16, 21, 25 idempotent in $\mathbb{Z}_{30}$

Part b

Define:

$$\begin{aligned}\varphi :\ \mathbb{Z}_{30} &\longrightarrow 6\mathbb{Z}_{30} \oplus 10\mathbb{Z}_{30} \oplus 15\mathbb{Z}_{30} \\ a &\mapsto (6a, 10a, 15a)\end{aligned}$$

Then:

$$\begin{aligned}a\varphi + b\varphi &= (6a, 10a, 15a) + (6b, 10b, 15b) \\ &= (6a + 6b, 10a + 10b, 15a + 15a) \\ &= (6(a+b), 10(a+b), 15(a+b)) \\ &= (a+b)\varphi\end{aligned}$$

$$\begin{aligned}(a\varphi)(b\varphi) &= (6a, 10a, 15a)(6b, 10b, 15b) \\ &= ((6a)(6b), (10a)(10b), (15a)(15a)) \\ &= (6^2(ab), 10^2(ab), 15^2(ab)) \\ &= (6(ab), 10(ab), 15(ab)) \text{ (as 6,10,15 idempotent)} \\ &= (ab)\varphi\end{aligned}$$

Thus φ is a homomorphism.

Now define:

$$\begin{aligned}\varphi^{-1} :\ 6\mathbb{Z}_{30} \oplus 10\mathbb{Z}_{30} \oplus 15\mathbb{Z}_{30} &\longrightarrow \mathbb{Z}_{30} \\ (6e, 10f, 15g) &\mapsto 6e + 10f + 15g\end{aligned}$$

Note in $\mathbb{Z}_{30}$:

$$\begin{aligned}(6)(10) = (10)(6) = 0 \\ (10)(15) = (15)(10) = 0 \\ (15)(6) = (6)(15) = 0\end{aligned}$$

Then:

$$\begin{aligned}((6e, 10f, 15g)\varphi^{-1})\varphi &= (6e + 10f + 15g)\varphi \\ &= (6(6e + 10f + 15g), 10(6e + 10f + 15g), 15(6e + 10f + 15g)) \\ &= (6^2e + 6(10)f + 6(15)g, 10(6)e + 10^2f + 10(15)g, 15(6)e + 15(10)f + 15^2g) \\ &= (6e, 10f, 15g)\end{aligned}$$

And if for $a, b \in \mathbb{Z}_{30}$:

$$\begin{aligned}&a\varphi = b\varphi \\ &\implies (6a, 10a, 15a) = (6b, 10b, 15b) \\ &\implies (6a = 6b) \wedge (10a = 10b) \wedge (15a = 15b)\end{aligned}$$

In $\mathbb{Z}_{30}$ this is only possible if $a = b$

Thus φ is a bijective as it is both injective and surjective.
Thus there exists a bijective homomorphism $\varphi :\ \mathbb{Z}_{30} \longrightarrow 6\mathbb{Z}_{30} \oplus 10\mathbb{Z}_{30} \oplus 15\mathbb{Z}_{30}$
Thus $\mathbb{Z}_{30} \cong 6\mathbb{Z}_{30} \oplus 10\mathbb{Z}_{30} \oplus 15\mathbb{Z}_{30}$ and $e = 6, f = 10, g = 30$

Part c

It is known that p, q coprime $\implies p\mathbb{Z}_{pq} = \mathbb{Z}_q$

Thus:

1. $6\mathbb{Z}_{30} \cong \mathbb{Z}_5$
2. $10\mathbb{Z}_{30} \cong \mathbb{Z}_3$
3. $15\mathbb{Z}_{30} \cong \mathbb{Z}_2$

And therefore:

$$\begin{aligned}\mathbb{Z}_{30} &\cong 6\mathbb{Z}_{30} \oplus 10\mathbb{Z}_{30} \oplus 15\mathbb{Z}_{30} \\ &\cong \mathbb{Z}_5 \oplus 10\mathbb{Z}_{30} \oplus 15\mathbb{Z}_{30} \\ &\cong \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus 15\mathbb{Z}_{30} \\ &\cong \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2\end{aligned}$$

It is also worth noting the Chinese Remainder Theorem:

$$p, q \text{ coprime} \implies \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

Thus as 2, 3, 5 prime:

$$\begin{aligned}\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 &\cong \mathbb{Z}_5 \oplus \mathbb{Z}_6 \\ &\cong \mathbb{Z}_{30} \text{ (as 5, 6 coprime)}\end{aligned}$$