THE UNIVERSITY OF SYDNEY

FACULTIES OF ARTS, ECONOMICS, EDUCATION,
ENGINEERING AND SCIENCE

MATH3066
ALGEBRA AND LOGIC

June 2016 Lecturer: David Easdown

Time allowed: two hours

No notes, books or calculators are allowed.

Instructions to candidates:

This examination paper comprises seven questions, each worth 20 marks.

The total number of marks available is 140.

Full marks may be awarded for achieving 120 or more marks.

All questions may be attempted.

Questions 1 *and* 2 *relate to the Propositional Calculus.*

Questions 3 *and* 4 *relate to the Predicate Calculus.*

Question 5 *relates to modular arithmetic.*

Questions 6 *and* 7 *relate to rings, integral domains and fields.*

For reference, on the last page of the examination paper, there is a list of the ten rules of deduction for the Propositional Calculus, followed by the further four rules of deduction for the Predicate Calculus.

1. (a) Give truth tables for each of the following, where P, Q and R are propositional variables:

$$\text{(i)} \quad P \Rightarrow (Q \vee R) \qquad\qquad \text{(ii)} \quad P \Rightarrow (Q \wedge R)$$

Make reference to relevant rows of your truth tables to explain briefly why

$$P \Rightarrow (Q \wedge R) \quad \models \quad P \Rightarrow (Q \vee R)\,,$$

but

$$P \Rightarrow (Q \vee R) \quad \not\models \quad P \Rightarrow (Q \wedge R)\,.$$

(b) Use truth values to verify that the following is a theorem in the Propositional Calculus:

$$\big(P \wedge R\big) \Rightarrow \Big(Q \vee \sim \big(P \Rightarrow (R \Rightarrow Q)\big)\Big)$$

(c) Use the formal rules of deduction of the Propositional Calculus (avoiding use of sequent or theorem introduction) to carefully prove the following sequents:

(i) $\quad P \Rightarrow (Q \wedge R) \;\vdash\; P \Rightarrow (Q \vee R)$

(ii) $\quad P \Rightarrow (Q \Rightarrow R)\;,\; \sim R \quad \vdash \quad Q \Rightarrow \sim P$

(iii) $\quad P \vee (Q \wedge R) \quad \vdash \quad (P \vee Q) \wedge (P \vee R)$

[20 marks]

2. (a) Consider any wff W in the Propositional Calculus. Let $\#W$ be the number of symbols that occur in W (including all brackets). Let $c(W)$ the number of occurrences of logical connectives $(\sim, \wedge, \vee, \Rightarrow, \Leftrightarrow)$ and $v(W)$ be the number of occurrences of propositional variables in W.

For example, if

$$W \;=\; \Big(\big((\sim P) \;\Leftrightarrow\; (Q \wedge P)\big) \;\Rightarrow\; \Big(R \vee\; \big(P \wedge\; (\sim Q)\big)\Big)\Big)$$

then $\#(W) = 27$, $c(W) = 7$ and $v(W) = 6$.

Prove, by induction on the length of a wff W, that

$$\#W \;=\; 3\,c(W) + v(W)\;.$$

(b) Let X, Y and Z be wffs built from propositional variables $P_1, P_2, \ldots, P_n$ (where n is a positive integer), and define the following wff (suppressing brackets in the usual way):

$$W_{X,Y,Z} \;:=\; \quad (X \Rightarrow \sim Y) \;\Rightarrow\; \sim (Z \Rightarrow X)\;.$$

(i) Use the truth table for implication to explain why

$$V(P \Rightarrow Q) \;=\; \begin{cases} V(\sim P) & \text{if } V(Q) = F, \\ \\ V(Q) & \text{if } V(P) = T. \end{cases}$$

(ii) Use part (i), or otherwise, to deduce that

$$V(W_{X,Y,Z}) \;=\; \begin{cases} V(Y) & \text{if } V(X) = T, \\ \\ V(Z) & \text{if } V(X) = F. \end{cases}$$

(iii) Suppose that $n \geq 2$ and Y and Z are built from variables $P_2, \ldots, P_n$ only. Denote the truth tables for Y and Z by $\mathcal{T}_Y$ and $\mathcal{T}_Z$ respectively. Describe the truth table for $W_{P_1,Y,Z}$ in terms of $\mathcal{T}_Y$ and $\mathcal{T}_Z$.

(iv) Use part (iii), or otherwise, to prove, by induction on n, that every truth table arises as the truth table of a wff built only using the logical connectives $\sim$ and $\Rightarrow$.

[20 marks]

3. (a) Use the rules of deduction of the Predicate Calculus to derive the following sequents (avoiding sequent or theorem introduction):

(i) $(\exists x)F(x)\,,\ (\forall x)\big(F(x) \Rightarrow G(x)\big) \ \vdash\ (\exists x)G(x)$

(ii) $(\exists x)(\forall y)\ H(x,y) \ \vdash\ (\forall y)(\exists x)\ H(x,y)$

(iii) $\sim (\forall x)F(x) \ \vdash\ (\exists x) \sim F(x)$

(b) Find faults in the following arguments:

(i) First faulty argument:

1	(1)	$\sim (\forall x) \sim G(x)$	A
2	(2)	$\sim\sim G(a)$	1 $\forall$ E
3	(3)	$G(a)$	2 DN
1	(4)	$(\exists x)G(x)$	3 $\exists$ I

(ii) Second faulty argument:

1	(1)	$\big((\exists x)F(x)\big) \Rightarrow \big((\exists y)G(y)\big)$	A
2	(2)	$\sim G(a)$	A
3	(3)	$F(a)$	A
3	(4)	$(\exists x)F(x)$	3 $\exists$ I
1, 3	(5)	$(\exists y)G(y)$	1, 4 MP
6	(6)	$G(a)$	A
2, 6	(7)	$G(a) \wedge \sim G(a)$	2, 6 $\wedge$ I
2, 6	(8)	$G(b) \wedge \sim G(b)$	7 SI(S) $(P \wedge \sim P \vdash Q)$
1, 2, 3	(9)	$G(b) \wedge \sim G(b)$	5, 6, 8 $\exists$ E
1, 2	(10)	$\sim F(a)$	3, 9 RAA
1	(11)	$\sim G(a) \Rightarrow \sim F(a)$	2, 10 CP
1	(12)	$(\forall x)(\sim G(x) \Rightarrow \sim F(x))$	11 $\forall$ I

(c) Find a model to demonstrate that the following sequent is not valid:

$$\big((\exists x)F(x)\big) \Rightarrow \big((\exists y)G(y)\big) \quad \vdash \quad (\forall x)(\sim G(x) \Rightarrow \sim F(x))$$

Briefly justify your answer.

[20 marks]

4. (a) Use the rules of deduction of the Predicate Calculus to derive the following sequent:

$$(\forall x)\big(F(x) \Rightarrow G(x)\big) \;\vdash\; (\forall z)\Big((\exists x)\big(F(x) \wedge H(x,z)\big) \;\Rightarrow\; (\exists y)\big(G(y) \wedge H(y,z)\big)\Big)$$

(b) Suppose that $\mathcal{U}$ is a model for the following wffs in the Predicate Calculus:

$$\begin{aligned} W_1 &:= (\exists x)(\exists y) \sim K(x,y) \;, \\ W_2 &:= (\forall x)(\forall y)\big(H(x,y) \Leftrightarrow \sim K(x,y)\big) \;, \\ W_3 &:= (\forall x)(\forall y)\big(H(x,y) \Rightarrow \sim H(y,x)\big) \;, \\ W_4 &:= (\forall x)(\forall y)\Big(K(x,y) \vee (\exists z)\big(H(y,z) \wedge H(z,x)\big)\Big) \;. \end{aligned}$$

(i) Explain why $\mathcal{U} \times \mathcal{U} = H \cup K$, and why this union is disjoint.

[Hint: consider W_2.]

(ii) Explain why the diagonal relation $\{(a,a) \mid a \in \mathcal{U}\}$ is contained in K.

[Hint: consider W_3 and apply part (i).]

(iii) Show that $\mathcal{U}$ has at least three distinct elements.

[Hint: consider W_1 and W_4, and apply part (ii).]

(iv) Find a model $\mathcal{U}$ for W_1, W_2, W_3, W_4 having exactly three elements, and show that in any such model H must consist of exactly three ordered pairs.

[20 marks]

5. (a) If $a, b \in \mathbb{Z}_n$ then we may write $\frac{a}{b} = c$ for some $c \in \mathbb{Z}_n$ if $bc = a$ in $\mathbb{Z}_n$ and c is unique with this property. In each case, evaluate the given fraction or explain why it does not exist:

(i) $\frac{2}{3}$ in $\mathbb{Z}_{13}$ (ii) $\frac{2}{3}$ in $\mathbb{Z}_{12}$ (iii) $\frac{6}{9}$ in $\mathbb{Z}_{12}$ (iv) $\frac{6}{9}$ in $\mathbb{Z}_{16}$

(b) Solve the following equations simultaneously over $\mathbb{Z}_{11}$ and explain why no solution exists over $\mathbb{Z}_{13}$:

$$\begin{aligned} 3x - y &= 2 \\ 7x + 2y &= 0 \end{aligned}$$

(c) Consider the ring

$$R = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

of remainders with addition and multiplication modulo the quadratic

$$p(x) = x^2 + 1 \,,$$

where all coefficients come from $\mathbb{Z}_3 = \{0, 1, 2\}$.

(i) Verify that $p(x)$ has no linear factors, so is irreducible. (Hence R is a field with 9 elements.)

(ii) Find a primitive element in R and explain why x is not primitive.

(iii) Find both square roots of x in R.

(iv) Solve over R the following quartic equation in α:

$$\alpha^4 + x\alpha^2 + 2 = 0 \,.$$

[20 marks]

6. (a) Use the ring axioms to verify that if R is a ring and if $a \in R$ then the negative of a is unique.

(b) Let R be a commutative ring with identity. Verify that R is an integral domain if and only if R is cancellative, that is

$$(\forall a, b, c \in R) \quad (a \neq 0) \wedge (ab = ac) \quad \Rightarrow \quad b = c \,.$$

You may use, without proof, the fact that $a \cdot 0 = 0$ for any $a \in R$.

(c) Give an example of an integral domain that is not a field.

(d) Let R be an integral domain, and define a relation $\sim$ on formal fractions as follows, where $a, b, c, d \in R$ and $b, d \neq 0$:

$$\frac{a}{b} \sim \frac{c}{d} \qquad \text{if and only if} \qquad ad = bc \,.$$

(i) Use cancellativity, or otherwise, to verify that $\sim$ is transitive.

(ii) Use $\sim$ to sketch the construction of the field of fractions F associated with R. In your sketch, explain briefly how multiplicative inverses of nonzero elements arise and how R embeds in F. You do not need to prove any assertions.

[20 marks]

7. (a) Prove carefully that if $\phi : R \to S$ is a ring homomorphism, where R and S are rings, then $0\phi = 0$ and $(a - b)\phi = a\phi - b\phi$ for all $a, b \in R$.

(b) Define what is meant by the *kernel*, denoted by $\ker \phi$, of a ring homomorphism $\phi : R \to S$, and verify that $\ker \phi$ is an ideal of R.

(c) State the Fundamental Homomorphism Theorem for rings.

(d) Define what is meant by the *direct sum* $R \oplus S$ of two rings R and S.

(e) Use the Fundamental Homomorphism Theorem, or otherwise, to prove that

$$\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x] \;\cong\; \mathbb{C} \quad \text{and} \quad \mathbb{R}[x]/(x^2 - 1)\mathbb{R}[x] \;\cong\; \mathbb{R} \oplus \mathbb{R}\,.$$

You may assume without proof that any appropriate polynomial evaluation map is a homomorphism.

(f) Prove that R and S are not isomorphic if R and S are distinct rings from the following list of quotient rings of $\mathbb{R}[x]$:

$$\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]\,, \quad \mathbb{R}[x]/(x^2 - 1)\mathbb{R}[x]\,, \quad \mathbb{R}[x]/x^2\mathbb{R}[x]\,.$$

[20 marks]

The Ten Rules of Deduction for the Propositional Calculus:

(1) **Rule of Assumptions (A):** Any wff may be written down as an assumption, depending only on itself.

(2) **Modus Ponens (MP):** Given V and $V \Rightarrow W$, we may deduce W, depending on the pooled assumptions for V and $V \Rightarrow W$.

(3) **Modus Tollens (MT):** Given $\sim W$ and $V \Rightarrow W$, we may deduce $\sim V$, depending on the pooled assumptions for $\sim W$ and $V \Rightarrow W$.

(4) **Double Negation (DN):** Given $\sim\sim W$, we may deduce W, and vice-versa, in each case depending on the same underlying assumptions.

(5) **Conditional Proof (CP):** Given V, introduced earlier by Rule of Assumptions, and given W, relying on V, we may deduce $V \Rightarrow W$, discharging V, but relying on any remaining assumptions used to deduce W from V.

(6) **$\wedge$-Introduction ($\wedge$ I):** Given V and W, we may deduce $V \wedge W$, relying on the pooled assumptions for V and W.

(7) **$\wedge$-Elimination ($\wedge$ E):** Given $V \wedge W$, we may deduce V or deduce W, relying on assumptions for $V \wedge W$.

(8) **$\vee$-Introduction ($\vee$ I):** Given V, we may deduce $V \vee W$ or deduce $W \vee V$ for any W, relying on the assumptions for V.

(9) **$\vee$-Elimination ($\vee$ E):** Given $V \vee W$ and two deductions of C, firstly from V, introduced by Rule of Assumptions, and secondly from W, introduced by Rule of Assumptions, we may deduce C again, but from $V \vee W$, discharging the assumptions V and W, but pooling any assumptions for $V \vee W$ and any assumptions used to deduce C from V and C from W.

(10) **Reductio ad Absurdum (RAA):** Given V, introduced earlier by Rule of Assumptions, and given the contradiction $W \wedge \sim W$, relying on V as an underlying assumption, we may deduce $\sim V$, discharging the assumption V, but relying on remaining assumptions used to deduce $W \wedge \sim W$ from V.

The Four Extra Rules of Deduction for the Predicate Calculus:

(11) **$\forall$-Introduction ($\forall$ I):** Given a wff $W(b)$, where b is a constant symbol that occurs at least once, we may deduce $(\forall x)\, W(x)$, where x is a new variable that does not appear in $W(b)$ and replaces b uniformly throughout $W(b)$, relying on the assumptions for $W(b)$, provided the symbol b does not appear in any wff in this list of underlying assumptions.

(12) **$\forall$-Elimination ($\forall$ E):** Given a wff $(\forall x)\, W(x)$, we may deduce $W(b)$, where b is a constant symbol replacing x uniformly throughout $W(x)$, relying on assumptions for $(\forall x)\, W(x)$.

(13) **$\exists$-Introduction ($\exists$ I):** Given a wff $W(b)$, where b is a constant that occurs at least once, we may deduce $(\exists x)\, W(x)$, where $W(x)$ results from $W(b)$ by replacing at least one occurrence of b by x, relying on assumptions for $W(b)$.

(14) **$\exists$-Elimination ($\exists$ E):** Given a wff $(\exists x)\, W(x)$ and a deduction of C from $W(b)$, introduced by Rule of Assumptions, where b is a new constant symbol that replaces x uniformly throughout $W(x)$, we may deduce C again, but from $(\exists x)\, W(x)$, discharging the assumption $W(b)$, but pooling any assumptions for $(\exists x)\, W(x)$ and any assumptions used to deduce C from $W(b)$, provided b does not appear in C or in any of these underlying assumptions.

THIS IS THE LAST PAGE OF THE EXAMINATION PAPER