Assignment 1

Mengxuan Wu

Q.1

(a)

$$p \land \neg q$$

(b)

$$p \to q$$

(c)

$$\neg p \to \neg q$$

(d)

$$p \to q$$

(e)

$$q \to p$$

Q.2

(a)

		$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$			
p	q	$\neg p$	$p \leftrightarrow q$	$\neg p \leftrightarrow q$	$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$
F	F	T	T	F	T
F	T	T	F	T	T
T	F	F	F	T	T
T	T	F	T	F	T

(b)

		$(p \oplus q) \wedge (p \oplus \neg q)$			
p	q	$\neg q$	$p \oplus q$	$p \oplus \neg q$	$(p \oplus q) \wedge (p \oplus \neg q)$
F	F	T	F	T	F
F	T	F	T	F	F
T	F	T	T	F	F
T	T	F	F	T	F

Q.3

(a)

Equivalent.

			$(p \to q) \vee (p \to r)$			$p \to (q \vee r)$	
p	q	r	$p \to q$	$p \to r$	$(p \to q) \vee (p \to r)$	$q \vee r$	$p \to (q \vee r)$
F	F	F	T	T	T	F	T
F	F	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	F	F	F	F	F
T	F	T	F	T	T	T	T
T	T	F	T	F	T	T	T
T	T	T	T	T	T	T	T

(b)

Not equivalent.

			$(p \to q) \to r$		$p \to (q \to r)$	
p	q	r	$p \to q$	$(p \to q) \to r$	$q \to r$	$p \to (q \to r)$
F	F	T	T	T	T	T
F	T	F	T	F	F	T
F	T	T	T	T	T	T
T	F	F	F	T	T	T
T	F	T	F	T	T	T
T	T	F	T	F	F	F
T	T	T	T	T	T	T

(c)

Equivalent.

			$(p \lor q) \to r$		$(p \to r) \land (q \to r)$		
p	q	r	$p \lor q$	$(p \lor q) \to r$	$p \to r$	$q \to r$	$(p \to r) \land (q \to r)$
F	F	F	F	T	T	T	T
F	F	T	F	T	T	T	T
F	T	F	T	F	T	F	F
F	T	T	T	T	T	T	T
T	F	F	T	F	F	T	F
T	F	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	T	T	T	T	T	T	T

Q.4

(a)

Proof.

$$\begin{aligned} \neg p \to (q \to r) &\equiv \neg p \to (\neg q \lor r) \\ &\equiv p \lor (\neg q \lor r) \\ &\equiv \neg q \lor (p \lor r) \\ &\equiv q \to (p \lor r) \end{aligned}$$

□

(b)

Proof.

$$\begin{aligned} (p \to q) \to ((r \to p) \to (r \to q)) &\equiv \neg(p \to q) \lor ((r \to p) \to (r \to q)) \\ &\equiv \neg(p \to q) \lor (\neg(r \to p) \lor (r \to q)) \\ &\equiv (\neg(p \to q) \lor \neg(r \to p)) \lor (r \to q) \\ &\equiv \neg((p \to q) \land (r \to p)) \lor (r \to q) \\ &\equiv \neg(r \to q) \lor (r \to q) \\ &\equiv T \end{aligned}$$

Since the statement is always true, it is a tautology. □

Q.5

Proof.

$$\begin{aligned}
(q \to (r \lor p)) \to ((\neg r \lor s) \land \neg s) &\equiv \neg(q \to (r \lor p)) \lor ((\neg r \lor s) \land \neg s) \\
&\equiv \neg(\neg q \lor (r \lor p)) \lor ((\neg r \lor s) \land \neg s) \\
&\equiv (q \land \neg(r \lor p)) \lor ((\neg r \lor s) \land \neg s) \\
&\equiv (q \land (\neg r \land \neg p)) \lor ((\neg r \lor s) \land \neg s) \\
&\equiv (\neg r \land (q \land \neg p)) \lor ((\neg r \lor s) \land \neg s) \\
&\equiv (\neg r \land (q \land \neg p)) \lor ((\neg r \land \neg s) \lor (s \land \neg s)) \\
&\equiv (\neg r \land (q \land \neg p)) \lor ((\neg r \land \neg s) \lor F) \\
&\equiv (\neg r \land (q \land \neg p)) \lor (\neg r \land \neg s) \\
&\equiv \neg r \land ((q \land \neg p) \lor \neg s)
\end{aligned}$$

The original statement implies $\neg r$ now becomes

$$\neg r \land ((q \land \neg p) \lor \neg s) \to \neg r$$

which is a tautology. (Simplification rule) □

Q.6

(a)

$$\forall x F(x, Fred)$$

(b)

$$\forall x \exists y F(x, y)$$

(c)

$$\neg \exists x \forall y F(x, y)$$

(d)

$$\forall y \exists x F(x, y)$$

(e)

$$\neg \exists x (F(x, Fred) \land F(x, Jerry))$$

(f)

$$\exists x \exists y (F(Nancy, x) \land F(Nancy, y) \land x \neq y \land \forall z (F(Nancy, z) \to (z = x \lor z = y)))$$

(g)

$$\exists y (\forall x F(x, y) \land \forall z (\forall x F(x, z) \to z = y))$$

(h)

$$\exists x \exists y (F(x,y) \land \forall z (F(x,z) \to z = y) \land x \neq y)$$

Q.7

(1)

$$\forall x \exists y \exists z Parent(y,x) \land Parent(z,x) \land x \neq y \land x \neq z \land y \neq z$$

(2)

$$Parent(x,y) \lor \exists z (Parent(z,y) \land Ancestor(x,z)) \to Ancestor(x,y)$$

Q.8

(a)

$$\begin{aligned}
\neg(\exists x \exists y P(x,y) \land \forall x \forall y Q(x,y)) &\equiv \neg \exists x \exists y P(x,y) \lor \neg \forall x \forall y Q(x,y) \\
&\equiv \forall x \forall y \neg P(x,y) \lor \exists x \exists y \neg Q(x,y)
\end{aligned}$$

(b)

$$\begin{aligned}
\neg(\forall x \exists y P(x,y) \lor \forall x \exists y Q(x,y)) &\equiv \neg \forall x \exists y P(x,y) \land \neg \forall x \exists y Q(x,y) \\
&\equiv \exists x \forall y \neg P(x,y) \land \exists x \forall y \neg Q(x,y)
\end{aligned}$$

(c)

$$\begin{aligned}
\neg(\forall x \exists y (P(x,y) \to Q(x,y))) &\equiv \neg \forall x \exists y (\neg P(x,y) \lor Q(x,y)) \\
&\equiv \exists x \forall y \neg(\neg P(x,y) \lor Q(x,y)) \\
&\equiv \exists x \forall y (P(x,y) \land \neg Q(x,y))
\end{aligned}$$

Q.9

Proof.

Step	Reason
1. $\exists x \forall y P(x,y)$	Premise
2. $\forall y P(x_0,y)$	Existential instantiation from 1
3. $P(x_0,y_0)$	Universal instantiation from 2
4. $\exists x P(x,y_0)$	Existential generalization from 3
5. $\forall y \exists x P(x,y)$	Universal generalization from 4

Hence, we can conclude that $\exists x \forall y P(x,y) \to \forall y \exists x P(x,y)$ is a tautology. □

Q.10

Let $Dis(x)$ means x has taken a course in discrete mathematics and $Alg(x)$ means x can take a course in algorithm. And we assume that the domain consists of all students. Then the premises can be written as:

$$\forall x(Dis(x) \to Alg(x)), Dis(A), Dis(B), Dis(C), Dis(D), Dis(E)$$

The process of deduction for A is as follows:

Step	Reason
1. $\forall x(Dis(x) \to Alg(x))$	Premise
2. $Dis(A) \to Alg(A)$	Universal instantiation from 1
3. $Dis(A)$	Premise
4. $Alg(A)$	Modus ponens from 2 and 3

Since this is true for each of A, B, C, D and E, we can conclude that

$$Alg(A) \land Alg(B) \land Alg(C) \land Alg(D) \land Alg(E) \qquad \text{(Reason: Conjunction)}$$

Q.11

(a)

Proof.

$$\begin{aligned}
P &\equiv \neg(p \leftrightarrow (q \lor \neg p)) \\
&\equiv \neg((p \land (q \lor \neg p)) \lor (\neg p \land \neg(q \lor \neg p))) \\
&\equiv \neg((p \land (q \lor \neg p)) \lor (\neg p \land (\neg q \land p))) \\
&\equiv \neg((p \land q) \lor (p \land \neg p) \lor ((\neg p \land p) \land \neg q)) \\
&\equiv \neg((p \land q) \lor F \lor (F \land \neg q)) \\
&\equiv \neg((p \land q) \lor F \lor F) \\
&\equiv \neg(p \land q) \\
&\equiv \neg p \lor \neg q
\end{aligned}$$

□

(b)

Proof.

		No T	one T				two Ts						three Ts				four Ts
p	q	$p \land \neg p$	$\neg p \land \neg q$	$\neg p \land q$	$p \land \neg q$	$p \land q$	$\neg p \land \neg p$	$\neg q \land \neg q$	$p \leftrightarrow q$	$\neg p \leftrightarrow q$	$q \land q$	$p \land p$	$\neg p \lor \neg q$	$\neg p \lor q$	$p \lor \neg q$	$p \lor q$	$p \lor \neg p$
F	F	F	T	F	F	F	T	T	T	F	F	F	T	T	T	F	T
F	T	F	F	T	F	F	T	F	F	T	T	F	T	T	F	T	T
T	F	F	F	F	T	F	F	T	F	T	F	T	T	F	T	T	T
T	T	F	F	F	F	T	F	F	T	F	T	T	F	T	T	T	T

As listed above, statement in the form of $A \square B$ can produce all possible truth tables consist of two atomic propositions, where $\square$ is one of $\land$, $\lor$, $\leftrightarrow$, and A and B are chosen from $\{p, \neg p, q, \neg q\}$. For each possible proposition P consist of atomic propositions p and q, we can find a statement $A \square B$ that has the same truth table as P, which means that P is logically equivalent to $A \square B$. □

Q.12

Disproof.
When $a = 2$ and $b = \frac{1}{2}$, $a^b = \sqrt{2}$ which is an irrational number. □

Q.13

(1)

Disproof.
When $a = e$ and $b = \ln 2$, $a^b = 2$ which is a rational number. □

(2)

Proof by contrapositive.
If $\sqrt{a}$ is a rational number, we can write $\sqrt{a} = \frac{m}{n}$ where $m, n \in Z$. Then we can infer that $a = (\sqrt{a})^2 = \frac{m^2}{n^2}$. Therefore, a is a rational number. □

Q.14

Proof by contradiction.
We assume that $\sqrt[3]{2}$ is a rational number. Then we can write $\sqrt[3]{2} = \frac{m}{n}$ where $m, n \in Z$. Without loss of generality, we assume that $\gcd(m, n) = 1$. Since $(\sqrt[3]{2})^3 = 2 = \frac{m^3}{n^3}$, we can infer that $m^3 = 2n^3$. Then m^3 is an even number, which means m is also an even number. Let $m = 2k$ where $k \in Z$, then $m^3 = 8k^3 = 2n^3$. Hence, we have $n^3 = 4k^3$, which means n^3 is an even number, which means n is also an even number. Since both m and n are even numbers, $\gcd(m, n)$ is at least 2, which contradicts with our original assumption. □

Q.15

Proof.

Lemma 1. *For any rational number r and any irrational number s, $r + s$ is irrational.*

Proof by contradiction.
We assume that $r + s$ is a rational number. Then we can write $r + s = \frac{m_1}{n_1} + s = \frac{m_2}{n_2}$ where $m_1, m_2, n_1, n_2 \in Z$. We can infer that $s = \frac{m_2}{n_2} - \frac{m_1}{n_1} = \frac{m_2 n_1 - m_1 n_2}{n_1 n_2}$, which means s is a rational number. This contradicts with our premise. □

Lemma 2. *For any rational number r and any irrational number s, $r \cdot s$ is irrational.*

Proof by contradiction.
We assume that $r \cdot s$ is a rational number. Then we can write $r \cdot s = \frac{m_1}{n_1} \cdot s = \frac{m_2}{n_2}$ where $m_1, m_2, n_1, n_2 \in Z$. We can infer that $s = \frac{m_2}{n_2} \cdot \frac{n_1}{m_1} = \frac{m_2 n_1}{m_1 n_2}$, which means s is a rational number. This contradicts with our premise. □

For any rational number a and b, assuming $a < b$ without loss of generality, we can always find a number $c = a + \frac{\sqrt{2}}{2}|a - b|$ that satisfies $a < c < b$. And since lemma 1 and lemma 2 have proved that the sum and product of a rational number and an irrational number is irrational, we can infer that c is an irrational number. □

Q.16

Proof by cases.
If $a^2 + b^2$ is even, then a^2 and b^2 must be both even or both odd, which means a and b must be both even or both odd.
Case 1: a and b are both even.
Let $a = 2m$ and $b = 2n$ where $m, n \in Z$, then $a + b = 2m + 2n = 2(m + n)$, which means $a + b$ is even.
Case 2: a and b are both odd.
Let $a = 2m+1$ and $b = 2n+1$ where $m, n \in Z$, then $a+b = 2m+1+2n+1 = 2(m+n+1)$, which means $a + b$ is even. □

Q.17

Proof by contradiction.
If one real root is neither an integer nor an irrational number, then it must be a fractional number. In that case, we assume that there exist two integers m and h such that $\gcd(m, h) = 1$ and $|h| \neq 1$ or 0, and the real root can be expressed as $\frac{m}{h}$. Then we can rewrite the equation as

$$\begin{aligned} f(\frac{m}{h}) &= a_0 + a_1\frac{m}{h} + a_2\frac{m^2}{h^2} + \cdots + a_{n-1}\frac{m^{n-1}}{h^{n-1}} + \frac{m^n}{h^n} \\ &= a_0 + \frac{a_1}{h}m + \frac{a_2}{h^2}m^2 + \cdots + \frac{a_{n-1}}{h^{n-1}}m^{n-1} + \frac{1}{h^n}m^n \\ &= 0 \end{aligned}$$

Then we move the last term $\frac{1}{h^n}m^n$ to the other side

$$-\frac{1}{h^n}m^n = a_0 + \frac{a_1}{h}m + \frac{a_2}{h^2}m^2 + \cdots + \frac{a_{n-1}}{h^{n-1}}m^{n-1}$$

We multiply both sides by h^n

$$\begin{aligned} -m^n &= a_0h^n + a_1h^{n-1}m + a_2h^{n-2}m^2 + \cdots + a_{n-1}hm^{n-1} \\ &= h(a_0h^{n-1} + a_1h^{n-2}m + a_2h^{n-3}m^2 + \cdots + a_{n-1}m^{n-1}) \end{aligned}$$

Since all variables are integers, $a_0h^{n-1} + a_1h^{n-2}m + a_2h^{n-3}m^2 + \cdots + a_{n-1}m^{n-1}$ is also an integer. This means h is a factor of m^n.
If we consider the prime factorization of h, we can write $|h| = p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$ where $p_1, p_2, \cdots, p_k$ are prime numbers and $f_1, f_2, \cdots, f_k$ are non-negative integers. Since $|h| \neq 1$ or 0, there must exist at least one f_i that is not equal to 0. Without loss of generality, we assume that $f_1 \neq 0$. Then we can infer that $p_1^{f_1}$ is a factor of m^n.

Lemma 3. *If a prime p is a factor of some power of an integer, then it is a factor of that integer.*

By lemma 3, we can infer that p_1 is also a factor of m, which means $\gcd(m, h) \geq p_1$ However, this contradicts with our original assumption that $\gcd(m, h) = 1$. $\square$