Homework 2 Solutions

Problem 1

Determine (with proof) if the following statements are true or false.

(a) $\exists x \in \mathbb{R}, e^x \leq 0$.

(b) $\forall n \in \mathbb{N}, \exists y \in \mathbb{R}, y = \sqrt{n}$.

(c) $\exists y \in \mathbb{R}, \forall n \in \mathbb{N}, y = \sqrt{n}$.

(d) $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}, mn = 1$.

(e) $\exists m \in \mathbb{Z}, \exists n \in \mathbb{Z}, mn = 1$.

(f) Let $F(\mathbb{R})$ be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$.

$$\forall f \in F(\mathbb{R}), [[(\forall a, b \in \mathbb{R}, f(a) = f(b) \Rightarrow a = b) \wedge (\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, f(x) = y)] \\ \Rightarrow [\exists g \in F(\mathbb{R}), \forall x, y \in \mathbb{R}, y = f(x) \Leftrightarrow x = g(y)]]$$

Suggested solutions:

(a) False: for any $x \in \mathbb{R}$, $e^x > 0$.

(b) True: the square root of any nonnegative real number (including natural number) is a real number.

(c) False: we show that $\forall y \in \mathbb{R}, \exists n \in \mathbb{N}, y \neq \sqrt{n}$. Let $y \in \mathbb{R}$. If $y = 0$, choose $n = 1$. Then $y = 0 \neq \sqrt{1} = \sqrt{n}$. If $y \neq 0$, choose $n = 0$, then $y \neq \sqrt{0} = \sqrt{n}$.

(d) False: we show that $\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, mn \neq 1$. Choose $m = 2$. The only real number n that makes $mn = 1$ is $n = 1/2 \notin \mathbb{Z}$.

(e) True: pick $m = n = 1 \in \mathbb{Z}$. We have $mn = 1$.

(f) (The formula is saying that if a function is bijective, then it has an inverse function.) We need to define $g \in F(\mathbb{R})$. It suffices to define the value of $g(b)$ for each $b \in \mathbb{R}$.
Let $b \in \mathbb{R}$. By the assumption $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, f(x) = y$, there is $a \in \mathbb{R}$ such that $f(a) = b$. We define $g(b) = a$. This ensures that $\forall x, y \in \mathbb{R}, y = f(x) \Leftrightarrow x = g(y)$.
It remains to check that g is actually in $F(\mathbb{R})$. We have given (at least) a value of g for each input $b \in \mathbb{R}$. We need to make sure that the value is unique. Let $b \in \mathbb{R}$. If we have given two values a_1, a_2 to $g(c)$, by our construction $f(a_1) = c = f(a_2)$. By the assumption $\forall a, b \in \mathbb{R}, f(a) = f(b) \Rightarrow a = b)$, we have $a_1 = a_2$. Therefore the value of $g(c)$ is unique.

Problem 2

For each of the following statements, write the logical negation in maximally negated form. Then decide which proposition (the original or the negation) is true, and why.

- Let $P(x)$ be the variable proposition "$1 \leq x \leq 3$"
- Let $R(x)$ be the variable proposition "$x^2 = 2$"
- Let $S(x)$ be the variable proposition "$x = 1$"

(a) $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}, (m \neq n \wedge P(m) \wedge R(n))$.

(b) $\forall n \in \mathbb{Z}, (R(n) \wedge S(n) \Rightarrow P(n) \wedge \neg P(n))$.

Suggested solutions:

(a)

$$\begin{aligned}
&\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, \neg(m \neq n \wedge (P(m) \wedge R(n)))\\
&\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, (m = n \vee \neg(P(m) \wedge R(n)))\\
&\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, (m = n \vee (\neg P(m) \vee \neg R(n)))\\
&\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, (m = n \vee ((x < 1) \vee (x > 3) \vee x^2 \neq 2))
\end{aligned}$$

The negation is true: pick $m = 1 \in \mathbb{Z}$ (this does not matter). For any $n \in \mathbb{Z}$, $x^2 \neq 2$ so $\neg R(n)$ is true.

(b)

$$\begin{aligned}
&\exists n \in \mathbb{Z}, \neg(R(n) \wedge S(n) \Rightarrow P(n) \wedge \neg P(n))\\
&\exists n \in \mathbb{Z}, (R(n) \wedge S(n) \wedge \neg(P(n) \wedge \neg P(n)))\\
&\exists n \in \mathbb{Z}, (R(n) \wedge S(n) \wedge (\neg P(n) \vee \neg\neg P(n)))\\
&\exists n \in \mathbb{Z}, (R(n) \wedge S(n) \wedge (\neg P(n) \vee P(n)))\\
&\exists n \in \mathbb{Z}, (x^2 = 2 \wedge x = 1 \wedge ((x < 1) \vee (x > 3) \vee 1 \leq x \leq 3))
\end{aligned}$$

The original proposition is true: let $n \in \mathbb{Z}$. We need to prove the implication $(R(n) \wedge S(n) \Rightarrow P(n) \wedge \neg P(n))$. It suffices to show that the antecedent $R(n) \wedge S(n)$ is false. If $S(n)$ holds, then $n = 1$, which makes $n^2 = 1 \neq 2$ so $R(n)$ fails.

Problem 3

Prove the following proposition:

prove that for all $m \in \mathbb{Z}$, m is odd if and only if 8 divides $m^2 - 1$.

Suggested solution:

Proof. Let $m \in \mathbb{Z}$. Assume m is odd, we need to prove that $8|m^2 - 1$. Write $m = 2k + 1$ for some $k \in \mathbb{Z}$. $m^2 - 1 = 4k^2 + 4k + 1 - 1 = 4(k^2 + k)$. It suffices to show that $k^2 + k$ is divisible by 2. If k is odd, then k^2 is also odd and $k^2 + k$ is even. If k is even, k^2 is also even and $k^2 + k$ is still even.
Assume $8|m^2 - 1$. We prove by contradiction that m is odd. Suppose m is even, then $m^2 - 1$ is an odd number, not divisble by 8, contradiction. Therefore, m is odd in the first place. $\square$

Problem 4

Use truth tables to determine whether or not the following statements are tautologies. p and q are arbitrary propositional variables.

(a) $((p \Rightarrow q) \wedge p) \Rightarrow q$

(b) $((p \Rightarrow q) \wedge \neg q) \Rightarrow \neg p$

(c) $(p \Rightarrow q) \vee (q \Rightarrow p)$

(d) $((p \Leftrightarrow q) \wedge p) \Leftrightarrow \neg q$

Suggested solutions:

(a) It is a tautology because the last column is all T.

p	q	$p \Rightarrow q$	$(p \Rightarrow q) \wedge p$	(a)
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

(b) It is a tautology because the last column is all T.

p	q	$p \Rightarrow q$	$\neg q$	$(p \Rightarrow q) \wedge \neg q$	$\neg p$	(b)
T	T	T	F	F	F	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

(c) It is a tautology because the last column is all T.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	(c)
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

(d) It is not a tautology because the last column is not all T.

p	q	$p \Leftrightarrow q$	$(p \Leftrightarrow q) \wedge p$	$\neg q$	(d)
T	T	T	T	F	F
T	F	F	F	T	F
F	T	F	F	F	T
F	F	T	F	T	F

Problem 5

(a) Let $a, b \in \mathbb{R}$ with $a < b$, and let $C[a, b]$ be the set of all continuous functions on the interval $[a, b]$.

Write a logical formula describing the Extreme Value Theorem. You are not allowed to use any English words in your logical formula.

(b) **Euclid's lemma**— If a prime p divides the product ab of two integers a and b, then p must divide at least one of those integers a or b.

Write a logical formula describing Euclid's lemma. You are not allowed to use any English words in your logical formula.

Suggested solutions:

(a) $\forall f \in C[a, b], \exists m, M \in [a, b], \forall x \in [a, b], (f(m) \leq f(x) \leq f(M))$

(b) $\forall a, b \in \mathbb{Z}, \forall p \in \mathbb{N}\Big(\big(p \neq 1 \wedge (\forall z \in \mathbb{N}, (\exists r \in \mathbb{Z}, rz = p) \Rightarrow (z = 1 \vee z = p)) \wedge$
$(\exists r \in \mathbb{Z}, ab = rp)\big) \implies ((\exists r \in \mathbb{Z}, a = rp) \vee (\exists r \in \mathbb{Z}, b = rp))\Big)$

Problem 6

Find a propositional formula φ whose truth table is as follows.

p	q	r	...	φ
T	T	T	...	F
T	T	F	...	T
T	F	T	...	F
T	F	F	...	F
F	T	T	...	T
F	T	F	...	F
F	F	T	...	F
F	F	F	...	F

The columns for the subformulae of φ should be included in your solution. Completing the truth table correctly (without extra justification) will be considered sufficient proof that your formula is correct, but you should indicate how you came up with your formula.

Suggested solution:

We use only the rows where φ is true. The formula is $(p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r)$.

p	q	r	$\neg r$	$p \wedge q \wedge \neg r$	$\neg p$	$\neg p \wedge q \wedge r$	φ
T	T	T	F	F	F	F	F
T	T	F	T	T	F	F	T
T	F	T	F	F	F	F	F
T	F	F	T	F	F	F	F
F	T	T	F	F	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	F	T	F	F
F	F	F	T	F	T	F	F

Problem 7 (Extra practice, not to be submitted)

(a) Use Euclid's Lemma to prove that:
For any prime p and for any integer a, p divides a^2 if and only if p divides a.

(b) Use the previous part to prove that: For any prime p, $\sqrt{p}$ is irrational.

Suggested solutions:

(a) Assume p divides a^2. By Euclid's Lemma, either p divides a or p divides a. Hence p divides a. Conversely, assume p divides a. There is $k \in \mathbb{Z}$ such that $a = pk$. Then $a^2 = p(pk^2)$. Since $pk^2 \in \mathbb{Z}$, p divides a^2.

(b) We prove by contradiction. Suppose there is a prime p such that $\sqrt{p}$ is rational. Then there are $m, n \in \mathbb{Z}$ coprime such that $\sqrt{p} = m/n$. Then $pn^2 = m^2$. Since $p|m^2$, by the previous part $p|m$. $p^2|m^2$ which means $p^2|pn^2$. We have $p|n^2$. By the previous part again $p|n$. This contradicts that m, n are coprime.