Sets, Logic and Categories
Solutions to Exercises: Chapter 3

3.1 This exercise gives a decision procedure for Hofstadter's MU-system (a rule for deciding whether or not a formula is a theorem of the system). Prove that a formula is a theorem of the system if and only if it has the properties

- its first letter is M, and all other letters are I or U;
- the number of occurrences of I is not divisible by 3.

An easy induction shows that the theorems of the MU-system satisfy the first condition, and we proved in Section 3.1 that they also satisfy the second condition.

So let ϕ be a formula which satisfies these two conditions. Let x and y be the numbers of occurrences of I and U in ϕ. Let 2^k be the smallest power of two such that $2^k > x+3y$ and 2^k is congruent to $x+3y$ mod 3. (By assumption, $x+3y$ is not divisible by 3; and powers of 2 are alternately congruent to 1 and 2 mod 3.)

Now start with MI. Applying Rule 2 k times gives M followed by 2^k Is. If $x+3y$ is odd, apply Rule 1 to add a U. Now apply Rule 3 repeatedly to replace the last $2^k-(x+3y)$ Is by $(2^k-(x+3y))/3$ Us, and Rule 4 to delete these Us (and the extra one if $x+3y$ is odd). This leaves M followed by $x+3y$ Is, from which Rule 3 applied y times in the appropriate places yields ϕ.

3.2 (a) Define a binary propositional connective $\downarrow$ with the following truth table:

ϕ	ψ	$(\phi\downarrow\psi)$
T	T	F
T	F	T
F	T	T
F	F	T

.

Prove that any propositional formula is logically equivalent to one using only this connective.

(b) Define another binary connective with this property.

(c) Show that, of the sixteen possible binary connectives which could be defined, only two have this property.

(a) It is enough to express negation and implication in terms of the connective $\downarrow$. Clearly $(\neg p)$ is equivalent to $(p\downarrow p)$, while $(p\to q)$ is equivalent to $(p\downarrow(\neg q))$.

(b) Define $\uparrow$ by the truth table

ϕ	ψ	$(\phi\uparrow\psi)$
T	T	F
T	F	F
F	T	F
F	F	T

.

The proof is similar.

(c) Any binary connective σ which suffices to express all truth functions must satisfy $(\mathsf{T}\,\sigma\,\mathsf{T}) = \mathsf{F}$: if not, then any function involving σ has the property that, if all its arguments are T, then the value is T. Similarly, it must satisfy $(\mathsf{F}\,\sigma\,\mathsf{F}) = \mathsf{T}$. This leaves just four possibilities.

If $(\mathsf{T}\,\sigma\,\mathsf{F}) = \mathsf{T}$ and $(\mathsf{F}\,\sigma\,\mathsf{T}) = \mathsf{F}$, then $(p\,\sigma\,q)$ is the same as $(\neg q)$, and a truth function expressed using σ depends only on its last argument. Similar reasoning deals with the case when $(\mathsf{T}\,\sigma\,\mathsf{F}) = \mathsf{F}$ and $(\mathsf{F}\,\sigma\,\mathsf{T}) = \mathsf{T}$.

The two remaining possibilities are $\downarrow$ and $\uparrow$.

3.3 (a) Show that $((\neg\psi) \to (\psi \to \theta))$ is a theorem.

(b) Show that, if both ψ and $(\neg\psi)$ can be deduced from $\Sigma \cup \{(\neg\phi)\}$, then ϕ can be deduced from Σ.

(c) Prove the following theorems:

(i) $(((\neg\phi) \to \psi) \to (((\neg\phi) \to (\neg\psi)) \to \phi))$;

(ii) $((\neg(\neg\phi)) \to \phi)$;

(iii) $((\phi \to \psi) \to ((\neg\psi) \to (\neg\phi)))$

(iv) $((\phi \to \psi) \to (((\neg\phi) \to \psi) \to \psi))$:

(v) $(\psi \to ((\neg\theta) \to (\neg(\psi \to \theta))))$.

You may have found this exercise very difficult. It includes all the theorems that we needed in the proof of the Completeness Theorem; so, once it is proved, it is never again necessary to devise a proof in propositional logic; simply compute a truth table.

The arguments given are skeletons of formal proofs.

(a) From the set $\{(\neg\psi)\}$, we can deduce

$$((\neg\theta) \to (\neg\psi))$$

(using (A1)), and then

$$(\psi \to \theta)$$

(using (A3)). The result now follows from the Deduction Theorem. This result tells us that, if we can deduce both ψ and $(\neg\psi)$, then we can deduce any formula (from the same hypotheses).

(b) Suppose that both ψ and $(\neg\psi)$ have been deduced from $\Sigma \cup \{(\neg\phi)\}$. Let α be any instance of an axiom. By (a), we can deduce $(\neg\alpha)$ from the same hypotheses. Hence, by the deduction theorem, from Σ we can deduce $((\neg\phi) \to (\neg\alpha))$, and hence also $(\alpha \to \phi)$ (by (A3)). Since α is an axiom, we can deduce ϕ.

(c) (i) From $(\neg\phi)$, $((\neg\phi) \to \psi)$ and $((\neg\phi) \to (\neg\psi))$, we can deduce both ψ and $(\neg\psi)$. By (b), we can deduce ϕ from the second and third hypotheses. The result now follows from two applications of the Deduction Theorem.

(ii) From $(\neg\phi)$ and $(\neg(\neg\phi))$ we can immediately deduce a proposition and its negation. By (b), we can deduce ϕ from $(\neg(\neg\phi))$. Now use the Deduction Theorem.

(iii) From $(\neg(\neg\phi))$, $(\phi \to \psi)$ and $(\neg\psi)$, we obtain ψ and its negation (using (ii)). So from the second and third hypotheses we get $(\neg\phi)$. Now use the Deduction Theorem.

(iv) Using (iii), from $(\phi \to \psi)$ and $((\neg\phi) \to \psi)$ we get $((\neg\psi) \to (\neg\phi))$ and $((\neg\psi) \to \phi)$, and hence ψ (using (i)). Now use the Deduction Theorem.

(v) From ψ we get $((\psi \to \theta) \to \theta)$, and hence $((\neg\theta) \to (\neg(\psi \to \theta)))$. Finish as usual.

3.4 Let $\phi_1, \ldots, \phi_n$ be formulae. Consider the 'pseudo-formula'

$$(\phi_1 \vee \phi_2 \vee \cdots \vee \phi_n).$$

It is possible to insert brackets to make this a well-formed formula in several different ways; for example, if $n = 3$,

$$((\phi_1 \vee \phi_2) \vee \phi_3) \text{ or } (\phi_1 \vee (\phi_2 \vee \phi_3)).$$

Show that, however the brackets are inserted, the truth value of the formula for any valuation is the same. (This justifies our cavalier misuse of brackets in the proof of the Four-Colour Theorem.)

The proof is by induction on n. For $n = 1$ and $n = 2$, there is nothing to prove, and the case $n = 3$ is the *distributive law*, which is easily verified by means of a truth table argument.

So suppose that $n > 3$, and assume that the result holds for all smaller values. We take two bracketings of $(\phi_1 \vee \phi_2 \vee \cdots \vee \phi_n)$, and look at the position of the next-to-outermost brackets: say

$$((\phi_1 \vee \phi_2 \vee \cdots \vee \phi_r) \vee (\phi_{r+1} \vee \phi_{r+2} \vee \cdots \vee \phi_n)),$$
$$((\phi_1 \vee \phi_2 \vee \cdots \vee \phi_s) \vee (\phi_{s+1} \vee \phi_{s+2} \vee \cdots \vee \phi_n)).$$

If $r = s$, then by the induction hypothesis, the first bracketed expressions on the two lines are equivalent, and so are the second bracketed expressions; so the whole formulae are equivalent.

Suppose that $r \neq s$; without loss of generality, suppose that $r < s$. By the induction hypothesis, we can re-bracket inside the left and right brackets in each line. Doing so, we can arrange that the next level of brackets are as follows in the two expressions:

$$((\phi_1 \vee \phi_2 \vee \cdots \vee \phi_r) \vee ((\phi_{r+1} \vee \phi_{r+2} \vee \cdots \vee \phi_s) \vee (\phi_{s+1} \vee \phi_{s+2} \vee \cdots \vee \phi_n))),$$
$$(((\phi_1 \vee \phi_2 \vee \cdots \vee \phi_r) \vee (\phi_{r+1} \vee \phi_{r+2} \vee \cdots \vee \phi_s)) \vee (\phi_{s+1} \vee \phi_{s+2} \vee \cdots \vee \phi_n)),$$

Now, by the induction hypothesis, each of the three bracketed terms in the first line is equivalent to the corresponding term in the second. By the distributive law, the two formulae are equivalent.

Remark: This argument shows that, in any system where the distributive law holds (for example, a group or a ring), the value of any n-fold composition is independent of the bracketing.

3.5 The following exercise outlines a proof that the Propositional Compactness Theorem, for any set of propositional variables, implies that every set can be totally ordered. Suppose that Propositional Compactness holds in general. Let X be a set, and take a family $\{p_{xy} : x,y \in X, x \neq y\}$ of propositional variables. Now let Σ consist of the following propositional formulae:

- $((p_{xy} \vee p_{yx}) \wedge (\neg(p_{xy} \wedge p_{yx})))$, for all distinct $x,y \in X$;
- $((p_{xy} \wedge p_{yz}) \to p_{xz})$, for all distinct $x,y,z \in X$.

Show that any finite subset of Σ is satisfiable. Show that a valuation v satisfying Σ gives rise to a total ordering of X by the rule that $x < y$ if and only if $v(p_{xy}) = \mathsf{T}$.

Consider a valuation v satisfying Σ. Define a relation $<$ on X by the rule that $x < y$ if and only if $x \neq y$ and $v(p_{xy}) = \mathsf{T}$. This relation is clearly irreflexive, antisymmetric, and transitive, and satisfies trichotomy; so it is a total order. Conversely, given any total order on X, if we define v by the rule that $v(p_{xy}) = \mathsf{T}$ if and only if $x < y$, then v satisfies Σ.

Now take any finite subset Σ_0 of Σ, and let X_0 be the set

$$\{x \in X : p_{xy} \text{ is contained in some formula in } \Sigma_0\}.$$

Then X_0 is finite, and so can be totally ordered; thus there is a valuation which satisfies Σ_0. By the Compactness Theorem, Σ is satisfiable, and we are done.

3.6 A *graph* consists of a set X of *vertices* with an irreflexive and symmetric relation R of *adjacency* on X. A *colouring* of a graph with a set C of colours is a function f from X to C with the property that, if x and y are adjacent vertices, then $f(x) \neq f(y)$. A *subgraph* of the graph (X,R) is a graph (Y,S), where $Y \subseteq X$ and $S = R \cap Y^2$.
Use the Compactness Theorem to prove that, if (X,R) is a graph whose vertex set X is well-ordered, and if every finite subgraph of the graph (X,R) has a colouring with a given finite set C of colours, then (X,R) has a colouring with this set of colours.

We follow the proof of the infinite four-colour theorem given in the text. Take a set $\{p_{x,c} : x \in X, c \in C\}$ of Boolean variables; this set is well-ordered since X is well-ordered and C is finite (Exercise 2.1). Now consider the following set Σ of formulae:

- For each $x \in X$, the (rather complicated) formula asserting that exactly one of the variables $\{p_{x,c} : c \in C\}$ takes the value T.
- $(\neg(p_{x,c} \wedge p_{y,c}))$, for all $(x,y) \in R$ and $c \in C$.

Now Σ is satisfiable if and only if the graph has a colouring with the set C of colours. So assume that every finite subgraph has a colouring with the set C of colours. Then every finite subset Σ_0 of Σ is satisfiable (since the subgraph consisting of all vertices $x \in X$ such that $p_{x,c}$ occurs in Σ_0 for some $c \in C$ is colourable). By the Compactness Theorem, Σ is satisfiable, amd we are done.

3.7 Prove Theorem 3.11.

This involves a lot of work with little reward. I will not give a solution here, but will provide one on request.

3.8 Let $P = \{p_1, \dots, p_n\}$ be a finite set of propositional variables, $V(P)$ the corresponding set of valuations, so that $|V(P)| = 2^n$. Let $V(P) = \{v_0, \dots, v_{2^n-1}\}$.

(a) Consider the set M of formulae which can be built using the connectives $\neg$ and $\leftrightarrow$ only. For any formula $\phi \in M$, let $x_0(\phi)$ be the number of occurrences of $\neg$ in ϕ, and $x_i(\phi)$ be the number of occurrences of p_i in ϕ for $i = 1, \dots, n$. Prove that a formula $\phi \in M$ is a tautology if and only if $x_i(\phi)$ is even for $i = 0, \dots, n$. Prove also that two formulae $\phi, \psi \in M$ are logically equivalent if and only if

$$x_i(\phi) \equiv x_i(\psi) \pmod 2$$

for $i = 0, \dots, n$.

(b) Prove that, if $\phi \in M$ is not a tautology or a contradiction, then $v(\phi) = \mathsf{T}$ for exactly half of the possible valuations $v \in V(P)$. Deduce that, if $\phi, \psi \in M$ and ψ is not equivalent to ϕ or $(\neg\phi)$, then $v(\phi) = v(\psi)$ for half the possible valuations $v \in V(P)$.

(c) Suppose that a transmitter A wants to send $n+1$ bits of information $(e_0, \dots, e_n)$ to a receiver B, over a noisy channel which will introduce some errors in the message. A chooses a formula $\phi \in M$ with $x_i(\phi) \equiv e_i \pmod 2$, and sends the sequence of 2^n values $v_i(\phi)$ for $v_i \in V(P)$. Show that, provided that fewer than one-quarter of the symbols are transmitted incorrectly, B can recover the information sent by A.

Represent the truth values T and F by 0 and 1 respectively, and let y_i be the value 0 or 1 corresponding to $v(p_i)$. (These values are taken in the binary field $\mathbb{Z}/(2)$.) If we let $f(\phi)$ be the value corresponding to $v(\phi)$, then we find that

$$f((\neg\phi)) = f(\phi) + 1, \qquad f((\phi \leftrightarrow \psi)) = f(\phi) + f(\psi).$$

Hence by induction

$$f(\phi) = a_0 + a_1 y_1 + \cdots + a_n y_n,$$

where $a_i = x_i(\phi)$. Now (a) follows, since ϕ is a tautology if and only if $f(\phi) = 0$.

(b) If ϕ is not a tautology but $x_0(\phi)$ is even, then $f(\phi)$ defines a linear map from $(\mathbb{Z}/(2))^n$ to $\mathbb{Z}/(2)$. Its kernel is a subspace of codimension one, and so contains half of the vectors. Adding 1 (that is, negating) has the effect of interchanging the values 0 and 1 taken by a formula, and again half the valuations will map it to zero. Now, given ϕ and ψ, the valuations v for which $v(\phi) = v(\psi)$ are just those for which $v((\phi \leftrightarrow \psi)) = \mathsf{T}$, which are half of all the valuations unless ψ is equivalent to ϕ or $(\neg\phi)$.

(c) Suppose that s errors occur. Then the received sequence differs from the correct one in s places. Also, since any two transmitted sequences differ in at least 2^{n-1} places, the received sequence differs from any other sequence in at least $2^{n-1} - s$ places. So, if $s < 2^{n-2}$, we can recognise the transmitted sequence as the unique one nearest to the received sequence.

3.9 The formal system for propositional logic given in this chapter has infinitely many axioms. Consider the following formal system, which has three axioms and two rules of inference. If ϕ and ψ are formulae and p is a propositional variable, let $\phi[\psi/p]$ denote the formula obtained from ϕ by substituting ψ for every occurrence of p.
The *axioms* are:

(A1) $(p_1 \to (p_2 \to p_1))$

(A2) $((p_1 \to (p_2 \to p_3)) \to ((p_1 \to p_2) \to (p_1 \to p_3)))$

(A3) $(((\neg p_1) \to (\neg p_2)) \to (p_2 \to p_1))$

The *rules of inference* are:

(MP) *Modus Ponens*: From ϕ and $(\phi \to \psi)$, infer ψ.

(S) *Substitution*: From ϕ, infer $\phi[\psi/p]$.

Prove that the Soundness and Completeness Theorem holds for this formal system.

Proof of soundness: Each of the axioms is a tautology: these axioms are particular cases of the axioms we used in the text. We also observed that Modus Ponens preserved truth. If ϕ is a tautology, it is true regardless of the truth value of p, and hence $\phi[\psi/p]$ is true regardless of the truth value which ψ takes under a given valuation. So Substitution also preserves tautologies.

Proof of completeness: From the three given axioms and the substitution rule, we immediately deduce the (infinitely many) axioms given in the text; so the proof of completeness given there applies.

3.10 Prove the Soundness and Completeness Theorem for the following *natural deduction system*: there are no axioms, and three rules of inference:

- *Modus Ponens*: from ϕ and $(\phi \to \psi)$, infer ψ;
- *Contradiction*: from $((\neg\phi) \to \psi)$ and $((\neg\phi) \to (\neg\psi))$, infer ϕ;
- *Deduction Theorem*: if ψ has been inferred from $\Sigma \cup \{\phi\}$, then infer $(\phi \to \psi)$ from Σ.

The proof of soundness (that the three rules preserve truth) is a simple truth table argument. For example, consider the Contradiction Rule. We have to show that, if a valuation v satisfies $v(((\neg\phi) \to \psi)) = v(((\neg\phi) \to (\neg\psi))) = \mathsf{T}$, then $v(\phi) = \mathsf{T}$. If the conclusion were false, then either $v(\psi)$ or $v((\neg\psi))$ would be F; and $v((\neg\phi)) = \mathsf{T}$, so the hypothesis is contradicted.

To prove completeness, it is enough to prove axioms (A1)–(A3). Here is the proof of (A3); the other two are similar but easier. From the hypotheses $\{((\neg\phi) \to (\neg\psi)), \psi, (\neg\phi)\}$ we can infer ψ. By the Deduction Theorem (which is a basic rule here, not a metatheorem!), from the set $\{((\neg\phi) \to (\neg\psi)), \psi\}$, we infer $((\neg\phi) \to \psi)$; and also, of course, $((\neg\phi) \to (\neg\psi))$. Now, by the Contradiction Rule, from the same hypotheses, we can infer ϕ. Two applications of the Deduction Theorem complete the proof.

3.11 Is there a sound and complete formal system for propositional logic with no rules of inference?

There is a formal system in which all tautologies are theorems: we simply take all tautologies as axioms. (Since tautologies are recognisable by the mechanical truth table method, this does indeed satisfy our definition of a formal system.) However, there is no such formal system in which all logical consequences of Σ are provable from Σ, for all sets Σ of formulae: without rules of inference we can prove nothing except axioms and members of Σ.

3.12 Logic is often regarded as the foundation on which mathematics is built. Are we justified, then, in using induction on the length of the formula ϕ in the proof of the Deduction Theorem?

This is not a question with a definite answer. My own view, as I hope the book makes clear, is that logic is a branch of mathematics, and the use of proof by induction in logic is no less valid than in, say, group theory or functional analysis. But you may wish to read the views of the various ‘schools’ of philosophy of mathematics and find out what their views would be. (The question was asked of me by a philosophy student in a lecture on propositional logic.)