CS1231S: Discrete Structures

Tutorial #1: Propositional Logic and Proofs

(Week 3: 26 – 30 August 2024)

Answers

Tutorials are meant to reinforce topics taught in lectures. Please try these questions on your own before coming to tutorial. In doing so, you may discover gaps in your understanding. Usually, a tutorial has a mix of easy, moderate and slightly challenging questions. It is perfectly fine if you cannot do some of the questions, but attempt them nonetheless, to at least get some partial solution.

You will be asked to present your answers. Your tutor's job is to guide you, not to provide the answers for you. Also, please keep in mind that the goal of tutorials is not to answer every question here, but to clarify doubts and reinforce concepts. Solutions to all tutorial questions will be given in the following week, but please treat them as a guide, for there are usually alternative ways of solving a problem.

You are also encouraged to raise your doubts or questions on **Canvas** or the **QnA** site https://sets.netlify.app/module/6698ae51322ba68d1103ffe8

Tutorials are important so attendance is taken and it contributes 5% of your final grade. If you miss a tutorial with valid reason (eg: due to illness), please submit your document (eg: medical certificate) to your respective tutor (softcopy or hardcopy) in advance or within 48 hours after your absence and you will not be penalized for your absence. You are to stick with your officially assigned tutorial group, or your attendance will not be taken. If you need to join a different group for just once with a valid reason, please email Aaron (tantc@comp.nus.edu.sg) in advance citing your reason, which is subject to approval.

Please take note of the above as it will not be repeated in subsequent tutorials.

Discussion Questions

The questions in this section will not be discussed in tutorial. You may discuss them or post your answer on Canvas or QnA.

D1. We discussed in class that English is an ambiguous language. Often, it also carries notions of perception, past experiences, cause and effect, etc. For example, in saying "today is rainy but hot", we use "but" because we often associate a rainy day as a cool day. In logic, there is no "but", "whenever", "unless", etc.; we need to find the appropriate logic connective. We would use "and" for "but" for the above example and write "today is rainy" ∧ "today is hot".

Let the statement variables p stand for "I went to Universal Studios Singapore" and q stand for "I rode the Battlestar Galactica". Express the following English statements into their respective logical compound statements.

(a) I did not go to Universal Studios Singapore.

(b) I went to Universal Studios Singapore but I did not ride the Battlestar Galactica.

(c) If I rode the Battlestar Galactica, then I did not go to Universal Studios Singapore,

(d) If I did not go to Universal Studios Singapore, then I did not ride the Battlestar Galactica.

(e) I went to Universal Studios Singapore or I rode the Battlestar Galactica.

(f) I went to Universal Studios Singapore or I rode the Battlestar Galactica, but not both.

(g) I did not go to Universal Studios Singapore or I went to Universal Studios Singapore and I rode the Battlestar Galactica.

D2. Draw a truth table to show that the following statement is a tautology:

$$\big((a \rightarrow x) \wedge (b \rightarrow y)\big) \rightarrow \big((a \wedge b) \rightarrow (x \wedge y)\big).$$

D3. Use the laws given in **Theorem 2.1.1 (Epp)** and the **implication law** to prove that the following are tautologies.

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

(b) $\big((p \vee q) \wedge {\sim}p\big) \rightarrow q$

(c) $\big((p \rightarrow q) \wedge p\big) \rightarrow q$

(d) $\big({\sim}p \rightarrow (q \wedge {\sim}q)\big) \rightarrow p$

Mathematical arguments are often constructed by using one implication (conditional statement) after another. Logically speaking, such an argument is constructed by using implications that are tautologies, like the ones above. For example, (c) is *modus ponens* and (d) is proof by contradiction. Part (b) is used in problems such as the Knights and Knaves.

D4. Mala has hidden her treasure somewhere on her property. She left a note in which she listed five statements (a-e below) and challenged the reader to use them to figure out the location of the treasure.

(a) If this house is next to a lake, then the treasure is not in the kitchen.

(b) If the tree in the front yard is an elm, then the treasure is in the kitchen.

(c) If the tree in the back yard is an oak, then the treasure is in the garage.

(d) The tree in the front yard us an elm or the treasure is buried under the flagpole.

(e) The house is next to a lake.

Where has Mala hidden her treasure?

II. Additional Notes

Given an argument:

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_k \\ \therefore q \end{array}$$

where $p_1, p_2, \dots, p_k$ are the k premises and q the conclusion, we can say that "the argument is valid if and only if $(p_1 \wedge p_2 \wedge \cdots \wedge p_k) \longrightarrow q$ is a tautology".

This serves as an alternative way to check whether an argument is valid, besides the critical row method shown in lecture. Go through the examples in the lecture yourself to verify the above.

III. Tutorial Questions

1. One of the most confusing concepts many students find is the difference between "if" and "only if", and the relationship among "if", "only if", "necessary condition" and "sufficient condition".

   a. Given these two statements: "I use the umbrella if it rains" and "I use the umbrella only if it rains". They may sound the same but in logic they are worlds apart! Now, rewrite them into propositional statements by using variable p for "I use the umbrella", variable q for "it rains" and the logical connective $\rightarrow$.

   b. "I use the umbrella if it rains": Is "I use the umbrella" a necessary condition for "it rains"? Or is "I use the umbrella" a sufficient condition for "it rains"? Is "it rains" a necessary condition for "I use the umbrella"? Or is "it rains" a sufficient condition for "I use the umbrella"?

   c. What if we say "I use the umbrella if and only if it rains"? How would you write a logic statement using variables p and q, the imply connective $\rightarrow$, and either $\wedge$ or $\vee$? Is there a shorter way to write the logic statement using some other logical connective?

   d. "I use the umbrella if and only if it rains". What kind of condition is "I use the umbrella" for "it rains"?

   Answers:

   a. "I use the umbrella if it rains" (is equivalent to "If it rains, then I use the umbrella"): $q \rightarrow p$

      "I use the umbrella only if it rains" (is equivalent to "if I use the umbrella, then it rains"): $p \rightarrow q$.

      "I use the umbrella only if it rains" is also equivalent to "if it doesn't rain, then I don't use the umbrella", which is $\sim q \rightarrow \sim p$, and we know it is equivalent to $p \rightarrow q$ by <u>contraposition</u>.

   b. "I use the umbrella if it rains": "I use the umbrella" is a <u>necessary condition</u> for "it rains". "It rains" is a <u>sufficient condition</u> for "I use the umbrella".

   c. "I use the umbrella if and only if it rains" is a conjunction of "I use the umbrella if it rains" and "I use the umbrella only if it rains", and hence the logic statement is $(q \rightarrow p) \wedge (p \rightarrow q)$ which can be shortened to $p \leftrightarrow q$.

      (From past experience, a number of students still did not know that $p \leftrightarrow q \equiv (q \rightarrow p) \wedge (p \rightarrow q)$ after several weeks of logic!)

d. "I use the umbrella if and only if it rains": "I use the umbrella" is a necessary and sufficient condition for "it rains".

2. The following are common mistakes made by students. Can you explain the mistakes and correct them?

   a. $a \wedge \sim(b \wedge c) \equiv a \wedge \sim b \vee \sim c$ by De Morgan's law

   b. $\sim(x \vee y) \vee z \equiv \sim x \wedge \sim y \vee z$ by De Morgan's law

   Answers:

   a. $a \wedge \sim b \vee \sim c$ is ambiguous!
   Corrected: $a \wedge \sim(b \wedge c) \equiv a \wedge (\sim b \vee \sim c)$

   b. $\sim x \wedge \sim y \vee z$ is ambiguous!
   Corrected: $\sim(x \vee y) \vee z \equiv (\sim x \wedge \sim y) \vee z$

3. Simplify the propositions below using the laws given in **Theorem 2.1.1 (Epp)** and the **implication law** (if necessary) with only negation ($\sim$), conjunction ($\wedge$) and disjunction ($\vee$) in your final answers. Supply a justification for every step.

   (For now, we want students to cite justification for every step. This is to ensure that you do not arrive at the answer by coincidence. Only after you have gained sufficient experience then would we relax this and allow you to skip obvious steps, or combine multiple steps in a line.)

   a. $\sim a \wedge \left(\sim a \rightarrow (b \wedge a)\right)$

   Aiken worked out his answer as shown below. However, he skipped some steps and hence his answer will not be awarded full credit. Can you point out the omissions? (Note: To show that two logical statements are equivalent, we use $\equiv$, not $=$.)

   $\sim a \wedge \left(\sim a \rightarrow (b \wedge a)\right)$
   $\equiv \sim a \wedge \left(a \vee (b \wedge a)\right)$ by the implication law
   $\equiv \sim a \wedge a$ by the absorption law
   $\equiv \textbf{false}$ by the negation law

   Reminder: We will use **true** and **false** instead of **t** and **c** (used in Susanna Epp's book) for tautology and contradiction respectively.

   b. $(p \vee \sim q) \rightarrow q$

   c. $\sim(p \vee \sim q) \vee (\sim p \wedge \sim q)$

   d. $(p \rightarrow q) \rightarrow r$

   Answers

   a. $\sim a \wedge \left(\sim a \rightarrow (b \wedge a)\right)$
   $\equiv \sim a \wedge \left(\sim(\sim a) \vee (b \wedge a)\right)$ by the implication law
   $\equiv \sim a \wedge \left(a \vee (b \wedge a)\right)$ by the ~~implication law~~ double negative law
   $\equiv \sim a \wedge \left(a \vee (a \wedge b)\right)$ by the commutative law
   $\equiv \sim a \wedge a$ by the absorption law
   $\equiv a \wedge \sim a$ by the commutative law
   $\equiv \textbf{false}$ by the negation law

b. $(p \vee {\sim}q) \rightarrow q$

$\equiv {\sim}(p \vee {\sim}q) \vee q$	by the implication law (step 1)
$\equiv \big({\sim}p \wedge {\sim}({\sim}q)\big) \vee q$	by De Morgan's law (step 2)
$\equiv ({\sim}p \wedge q) \vee q$	by the double negative law (step 3)
$\equiv q \vee ({\sim}p \wedge q)$	by the commutative law (step 4)
$\equiv q \vee (q \wedge {\sim}p)$	by the commutative law (step 5)
$\equiv q$	by the absorption law (step 6)

You don't need to write "step x".
This is for ease of explanation below.

Check:

- Did you jump from step 1 straight to step 3 by citing only the De Morgan's law but omitting the double negative law?
- Did you jump from step 3 straight to step 6 by skipping the two steps involving commutative law?

Also, remember to add appropriate parenthesis to avoid ambiguous statements. For example, from ${\sim}(p \vee {\sim}q) \vee q$ (step 1) to $\big({\sim}p \wedge {\sim}({\sim}q)\big) \vee q$ (step 2), if step 2 were written as ${\sim}p \wedge {\sim}({\sim}q) \vee q$, it would become an ambiguous statement since $\wedge$ and $\vee$ are coequal in precedence.

c. ${\sim}(p \vee {\sim}q) \vee ({\sim}p \wedge {\sim}q)$

$\equiv ({\sim}p \wedge {\sim}({\sim}q)) \vee ({\sim}p \wedge {\sim}q)$	by De Morgan's law
$\equiv ({\sim}p \wedge q) \vee ({\sim}p \wedge {\sim}q)$	by the double negative law
$\equiv {\sim}p \wedge (q \vee {\sim}q)$	by the distributive law
$\equiv {\sim}p \wedge \mathbf{true}$	by the negation law
$\equiv {\sim}p$	by the identity law

d. $(p \rightarrow q) \rightarrow r$

$\equiv ({\sim}p \vee q) \rightarrow r$	by the implication law
$\equiv ({\sim}({\sim}p \vee q)) \vee r$	by the implication law
$\equiv ({\sim}({\sim}p) \wedge {\sim}q) \vee r$	by De Morgan's law
$\equiv (p \wedge {\sim}q) \vee r$	by the double negative law

4. Prove, or disprove, that $(p \rightarrow q) \rightarrow r$ is logically equivalent to $p \rightarrow (q \rightarrow r)$.

Answers

$(p \rightarrow q) \rightarrow r$ is <u>not</u> logically equivalent to $p \rightarrow (q \rightarrow r)$.

Counterexample: Let p, q and r be false. Then $(p \rightarrow q) \rightarrow r$ is false but $p \rightarrow (q \rightarrow r)$ is true.

For such questions, sometimes you do not know whether the given statement is true or false. In this case, you would probably have to do some trial-and-errors, or to fill in the truth table:

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

You can see that there are two counterexamples, the sixth and eighth rows.

Certainly, filling out the whole truth table is tedious and should be avoided.

5. Given the conditional statement "If $12x - 7 = 29$, then $x = 3$", write the **negation**, **contrapositive**, **converse** and **inverse** of the statement.

Is the given conditional statement true? If it true, prove it; otherwise, give a counter-example.

Is its converse true? If it is true, prove it; otherwise, give a counter-example.

In general, is it possible for the converse of a conditional statement to be true while the inverse of the same statement is false? Why?

Answers

Negation: $12x - 7 = 29$ and $x \neq 3$.
Contrapositive: If $x \neq 3$, then $12x - 7 \neq 29$.
Converse: If $x = 3$, then $12x - 7 = 29$.
Inverse: If $12x - 7 \neq 29$, then $x \neq 3$.
Both the given conditional statement and its converse are true.

Proof for "If $12x - 7 = 29$, then $x = 3$":

1. $12x - 7 = 29$ (given)
2. Then $12x = 29 + 7 = 36$ (by basic algebra)
3. Then $x = 3$ (by basic algebra)

Proof for "If $x = 3$, then $12x - 7 = 29$":

1. Substitute $x = 3$ into $12x - 7 = 29$
2. $12(3) - 7 = 36 - 7 = 29$ (by basic algebra)

It is not possible for the converse of a conditional statement to be true while the inverse of the same statement is false, as the converse is logically equivalent to the inverse of a statement.

6. The conditional statement $p \to q$ is an important logical statement. Recall that it is defined by the following truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Oftentimes, students are perplexed by this definition. The first two rows look reasonable, but the last two rows seem strange. However, this way of defining $p \to q$ actually gives us the nice intuitive property of the following statement:

$$\big((p \to q) \land (q \to r)\big) \to (p \to r)$$

which is the **transitive rule of inference** we studied in lecture (Lecture #2, slide 65):

$$\begin{array}{l} \quad p \to q \\ \quad q \to r \\ \therefore p \to r \end{array}$$

For example, given premises "if x is a square then x is a rectangle" and "if x is a rectangle than x is a quadrilateral", the conclusion is "if x is a square then x is a quadrilateral". We use such intuitive reasoning very often in our life.

Show that if we define the conditional statement alternatively as follows, then the transitive rule of inference would no longer hold.

Alternative 1: $\to_a$

p	q	$p \to_a q$
T	T	T
T	F	F
F	T	F
F	F	F

Alternative 2: $\to_b$

p	q	$p \to_b q$
T	T	T
T	F	F
F	T	T
F	F	F

Alternative 3: $\to_c$

p	q	$p \to_c q$
T	T	T
T	F	F
F	T	F
F	F	T

Answers

Alternative 1: $\rightarrow_a$

p	q	r	$p \rightarrow_a q$	$q \rightarrow_a r$	$p \rightarrow_a r$	$(p \rightarrow_a q) \wedge (q \rightarrow_a r)$	$\big((p \rightarrow_a q) \wedge (q \rightarrow_a r)\big) \rightarrow_a (p \rightarrow_a r)$
T	T	F	T	F	F	F	F

Therefore, $\big((p \rightarrow_a q) \wedge (q \rightarrow_a r)\big) \rightarrow_a (p \rightarrow_a r)$ is not a tautology.

Alternative 2: $\rightarrow_b$

p	q	r	$p \rightarrow_b q$	$q \rightarrow_b r$	$p \rightarrow_b r$	$(p \rightarrow_b q) \wedge (q \rightarrow_b r)$	$\big((p \rightarrow_b q) \wedge (q \rightarrow_b r)\big) \rightarrow_b (p \rightarrow_b r)$
T	T	F	T	F	F	F	F

Therefore, $\big((p \rightarrow_b q) \wedge (q \rightarrow_b r)\big) \rightarrow_b (p \rightarrow_b r)$ is not a tautology.

Alternative 3: $\rightarrow_c$

p	q	r	$p \rightarrow_c q$	$q \rightarrow_c r$	$p \rightarrow_c r$	$(p \rightarrow_c q) \wedge (q \rightarrow_c r)$	$\big((p \rightarrow_c q) \wedge (q \rightarrow_c r)\big) \rightarrow_c (p \rightarrow_c r)$
F	T	F	F	F	T	F	F

Therefore, $\big((p \rightarrow_c q) \wedge (q \rightarrow_c r)\big) \rightarrow_c (p \rightarrow_c r)$ is not a tautology.

7. Some of the arguments below are valid, whereas others exhibit the converse or inverse error. Use symbols to write the logical form of each argument. If the argument is valid, identify the rule of inference that guarantees its validity. Otherwise, state whether the converse or the inverse error is made.

   a. Sandra knows Java and Sandra knows C++.
      ∴ Sandra knows C++.

   b. If at least one of these two numbers is divisible by 6, then the product of these two numbers is divisible by 6.
      Neither of these two numbers is divisible by 6.
      ∴ The product of these two numbers is not divisible by 6.

   c. If there are as many rational numbers as there are irrational numbers, then the set of all irrational numbers is infinite.
      The set of all irrational numbers is infinite.
      ∴ There are as many rational numbers as there are irrational numbers.

   d. If I get a Christmas bonus, I'll buy a stereo.
      If I sell my motorcycle, I'll buy a stereo.
      ∴ If I get a Christmas bonus or I sell my motorcycle, I'll buy a stereo.

Answers

a. Let p be "Sandra knows Java".
   Let q be "Sandra knows C++".
   $p \wedge q$ (premise)
   $\therefore q$ (valid by specialization)

b. Let p be "the first number is divisible by 6.".
   Let q be "the second number is divisible by 6".
   Let r be "the product of these two numbers is divisible by 6".
   $p \vee q \rightarrow r$ (premise)
   $\sim p \wedge \sim q$ (premise)
   $\therefore \sim r$ (invalid: inverse error; explicit counter-example: 2 and 3)
   Note that such a deduction is invalid even if there are no counter-examples.

c. Let p be "there are as many rational numbers as there are irrational numbers".
   Let q be "the set of all irrational numbers is infinite".
   $p \rightarrow q$ (premise)
   q (premise)
   $\therefore p$ (invalid: converse error; in fact, p is false, but both premises are true)

d. Let p be "I get a Christmas bonus".

Let q be "I sell my motorcycle".

Let r be "I'll buy a stereo".

$p \rightarrow r$	(premise)
$q \rightarrow r$	(premise)
$(p \rightarrow r) \wedge (q \rightarrow r)$	(conjunction of premises)
$(\sim p \vee r) \wedge (\sim q \vee r)$	(implication law)
$(r \vee \sim p) \wedge (r \vee \sim q)$	(commutative law)
$r \vee (\sim p \wedge \sim q)$	(distributive law)
$(\sim p \wedge \sim q) r \vee r$	(commutative law)
$\sim (p \vee q) \vee r$	(De Morgan's law)
$\therefore (p \vee q) \rightarrow r$	(implication law)

8a. Given the following argument:

$p \vee (q \wedge r)$

$\sim p$

$\therefore q \wedge r$

<u>Without</u> actually drawing the truth table, determine the values of p, q and r in the critical row(s) of the truth table. Is the argument valid?

b. Give a counterexample to show that the following argument is invalid.

$p \vee (q \wedge r)$

$\sim (p \wedge q)$

$\therefore r$

c. Determine whether the following argument is valid or invalid. Use variables to represent the statements (for example: let p be "I go to the beach".)

If I go to the beach, I will take my shades or my sunscreen.

I am taking my shades but not my sunscreen.

∴ I will go to the beach.

d. Determine whether the following argument is valid or invalid. Use variables to represent the statements.

I will buy a new goat or a used Yugo.

If I buy both a new goat and a used Yugo, I will need a loan.

I bought a used Yugo but I don't need a loan.

∴ I didn't buy a new goat.

Answers

a. Critical rows are those where the premises are true. Therefore, we can use deduction here instead of drawing the whole truth table. Here, the two premises are $p \vee (q \wedge r)$ and $\sim p$. So, p must be false and hence both q and r must be true. There is one critical row and the conclusion $q \wedge r$ in that row is true. Therefore, the argument is **valid**.

b. Counterexample: $p \equiv true, q \equiv r \equiv false$.
Both premises $p \vee (q \wedge r)$ and $\sim(p \wedge q)$ are true, but the conclusion r is false.

c. Let p be "I go to the beach"; q be "I take my shades"; and r be "I take my sunscreen".

$$p \rightarrow q \vee r$$
$$q \wedge \sim r$$
$$\therefore p$$

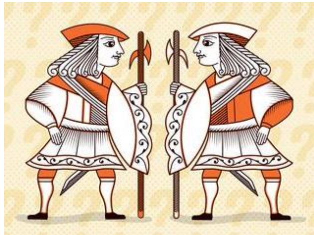
Critical row: $p \equiv false;\ q \equiv true;\ r \equiv false$. Conclusion: false.
Therefore, the argument is **invalid**.

d. Let p be "I buy a new goat"; q be "I buy a used Yugo"; and r be "I need a loan".

$$p \vee q$$
$$(p \wedge q) \rightarrow r$$
$$q \wedge \sim r$$
$$\therefore \sim p$$

Critical row: $p \equiv false;\ q \equiv true;\ r \equiv false$. Conclusion: true.
Therefore, the argument is **valid**.

9. The island of Wantuutrewan is inhabited by exactly two types of people: **knights** who always tell the truth and **knaves** who always lie. Every native is a knight or a knave, but not both. You visit the island and have the following encounters with the natives.



a. Two natives *A* and *B* speak to you:

A says: Both of us are knights.
B says: *A* is a knave.

What are *A* and *B*?

b. Two natives *C* and *D* speak to you:

C says: *D* is a knave.
D says: *C* is a knave.

How many knights and knaves are there?

Part (a) has been solved for you (see below). Study the solution, and use the same format in answering part (b).

Answer for part (a):

Proof (by contradiction).

1. If *A* is a knight, then:

1.1	What *A* says is true.	(by definition of knight)
1.2	∴ *B* is a knight too.	(that's what *A* says)
1.3	∴ What *B* says is true.	(by definition of knight)
1.4	∴ *A* is a knave.	(that's what *B* says)
1.5	∴ *A* is not a knight.	(since *A* is either a knight or a knave, but not both)
1.6	∴ Contradiction to 1.	

2.	∴ *A* is not a knight.	
3.	∴ *A* is a knave.	(since *A* is either a knight or a knave, but not both)
4.	∴ What *B* says is true.	
5.	∴ *B* cannot be a knave.	(as *B* has said something true)
6.	∴ *B* is a knight.	(one is a knight or a knave)
7.	Conclusion: *A* is a knave and *B* is a knight.	

Notes:

- It is tempting to say "Contradiction" right after line 1.4. However, this is not valid because contradiction requires $p \wedge {\sim}p$, but 'knave' is not the negation of 'knight'. Hence line 1.5 is required before we arrive at the contradiction in 1.6.

Answer

b. Proof (by division into cases)

1. If *C* is a knight:
   1.1 What *C* says is true. (by definition of knight)
   1.2 ∴ *D* is a knave. (that's what *C* says)
2. If *C* is not a knight:
   2.1 Then *C* is a knave. (one is either a knight or a knave)
   2.2 ∴ what *C* says is false. (by definition of knave)
   2.3 ∴ *D* is not a knave. (*C* says *D* is a knave, but what *C* says is false)
   2.4 ∴ *D* is a knight. (one is either a knight or a knave)
3. In both cases, there is one knight and one knave.

10. Recall the definitions of even and odd integers in Lecture #1 slide 27:

> If n is an integer, then
> n is even if and only if $\exists k \in \mathbb{Z}$ s.t. $n = 2k$;
> n is odd if and only if $\exists k \in \mathbb{Z}$ s.t. $n = 2k + 1$.

Prove the following:

The product of any two odd integers is an odd integer.

Answer

Proof (direct proof).

1. Take <u>any</u> two odd integers n, m. (Note: This means ∀ odd integers n, m)
2. Then $n = 2k + 1$ and $m = 2p + 1$ for $k, p \in \mathbb{Z}$ (by definition of odd integers).
3. Hence $nm = (2k + 1)(2p + 1) = \big(2k(2p + 1)\big) + (2p + 1)$
   $= (4kp + 2k) + (2p + 1) = 2(2kp + k + p) + 1$ (by basic algebra)
4. Let $q = 2kp + k + p$ which is an integer (by closure of integers under $+$ and $\times$)
5. Then $nm = 2q + 1$ which is odd (by definition of odd integers).
6. Therefore, the product of any two odd integers is an odd integer.

(Reminder: Did you write the justification for every important step?)

11. Your classmate Smart came across this claim:

Let n be an integer. Then n^2 is odd if and only if n is odd.

a. Smart attempts to prove the above claim as follows:

Proof (by contradiction).

1. Suppose n is an even integer.
2. Then $\exists k \in \mathbb{Z}$ s.t. $n = 2k$.
3. Squaring both sides, we get $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.
4. Since k is an integer, so is $2k^2$.
5. Hence $n^2 = 2p$, with $p = 2k^2 \in \mathbb{Z}$.
6. Therefore, n^2 is even.
7. So, if n is even, then n^2 is even, which is the same as saying, if n^2 is odd, then n is odd.
8. Therefore, n^2 is odd if and only if n is odd.

Comment on Smart's proof.

b. Write your own proof.

Answers

a. There are several things that Smart did not do right:
   - He is proving the contrapositive of "if n^2 is odd, then n is odd", so it is only one direction.
   - He wrote "proof (by contradiction)", which is wrong. It should be proof by contraposition.
   - No justification at a few places. For example, step 2 (by definition of an even integer), step 4 (by closure of integers under multiplication), and step 6 (by definition of an even integer).

b. Proof:

1. ($\Rightarrow$) Proving the contraposition of "if n^2 is odd, then n is odd".
   - 1.1. Suppose n is even.
   - 1.2. Then $\exists k \in \mathbb{Z}$ s.t. $n = 2k$. (by definition of even integers)
   - 1.3. Squaring both sides, we get $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. (by basic algebra)
   - 1.4. Hence $n^2 = 2p$, with $p = 2k^2 \in \mathbb{Z}$. (by closure of integers under $\times$)
   - 1.5. Therefore, n^2 is even. (by definition of even integers)
   - 1.6. This proves that if n^2 is odd, then n is odd.
2. ($\Leftarrow$) If n is odd, then $n \times n = n^2$ is odd. (by question 10)
3. Therefore, n^2 is odd if and only if n is odd. (by lines 1.6 and 2)