AA1H, Solutions to Assignment 1

• Read again the remarks with the original assignment which discuss how to set out a proof.
• If your proofs were much longer than those given here, think carefully about how you could shorten them. What were the critical points in your proof?
• Carefully study the *Remarks* made here after the solutions, even if you received close to full grade. The errors and points of logic I discuss are very important, not only in this assignment but also throughout the course.
• Only Exercises 4 and 6 will be graded, and tyou wil receive a grade out of 10.
• You will also receive a separate grade out of 10 for mathematical precision and style. This is for you own inforamtion, and is of necessity a little arbitrary. I will keep a record, but it will NOT be used in any way in your final grade.

Roughly Speaking

Score	*Remarks*
1–2	Stream of consciousness, reads like "Finnegan's Wake"
3–4	Not clear what is being assumed, nor what follows from what
5–7	Make sure you use connecting words such as "implies", "if", "we assume" "in order to get a contradiction, we assume", "therefore", etc. Do not forget to state your assumptions clearly. Keep the arguments reasonably brief, about the length of the example solutions.
8–9	Very good, well set out, but still capable of some improvement, see the example solutions
10	Excellent

Exercise 1. Read Sections 2.1–2.3, Section 2.5 to the beginning of Theorem 2.12, and Section 2.6.

Exercise 2. Prove from the axioms that *if* a, b *and* c *are real numbers,* $c \neq 0$, *and* $ac = bc$, *then* $a = b$. HINT: Use an argument similar to that in Theorem 2.2.

Solution. Assume

$$ac = bc$$

and $c \neq 0$. Since ac and bc are equal, we obtain the same number if we multiply ac by c^{-1} or bc by c^{-1}; i.e.

$$(ac)c^{-1} = (bc)c^{-1}.$$

(This uses the existence of the number c^{-1} from A8.) Hence

$$a(cc^{-1}) = b(cc^{-1})$$

from A6 applied twice, once to each side of the equation. Hence

$$a1 = b1$$

from A8 applied twice. Finally,

$$a = b$$

from A7. □

Remark. A common mistake was to write acc^{-1} instead of $(ac)c^{-1}$. The problem is that acc^{-1} can mean *either* $a(cc^{-1})$ *or* $(ac)c^{-1}$. Of course, these are equal, but *that* is a fact that requires the associative axiom, and the use of the associative axiom should be explicitly noted. In this question where you were asked to justify everything in term of the axioms, and you should put in brackets to remove any ambiguity.

Exercise 3. Prove from the axioms that for any number a, $a0 = 0$. HINT: This is just Theorem 2.3.2, and is done on page 18. So all you have to do is to justify the 4 steps in terms of the axioms, rules of logic, or something else already proved from the axioms.

Solution. The trick here is to use the fact $0 + 0 = 0$ (from A3), together with the distributive axiom A9. The proof is as follows:
One has $a(0 + 0) = a0$ (since $0 + 0 = 0$ from A4)
But the left side equals $a0 + a0$ (from A9)
and the right side equals $0 + a0$ (from A4)
Hence $a0 + a0 = 0 + a0$
Hence $a0 = 0$ (from Theorem 2.2). □

Exercise 4.
1. Prove from the axioms that $a + (b - a) = b$. *HINT*: What was the definition of $b - a$?
2. Prove from the axioms that *if* $a + x = b$ *then* $x = b - a$.
   The first part of the question shows that $b - a$ is *a* solution of $a + x = b$. The second part shows that it is the *only* solution. Notice this subtle but important distinction.
3. Deduce that 0 is the *only* real number that has the property $a+0 = 0+a = a$. for all a.

Solution.
1.

$$
\begin{aligned}
a + (b - a) &= a + (b + (-a)) \quad \text{by the definition of } b - a \\
&= a + ((-a) + b) \quad \text{by the commutative axiom for } + \\
&= (a + (-a)) + b \quad \text{by the associative axiom for } + \\
&= 0 + b \quad \text{by the additive inverse axiom} \\
&= b \quad \text{by the identity axiom for } +
\end{aligned}
$$

2. *Assume* that $a + x = b$ (where as usual, a, b and x are real numbers). Hence

$$(a + x) + (-x) = b + (-x)$$

as we are adding the same number $-x$ to each side of the original equality being assumed. Hence

$$a + (x + (-x)) = b - x$$

by the associative axiom on the left side and the definition of $b - x$ on the right side. Hence

$$a + 0 = b - x$$

by the additive inverse axiom, and so

$$a = b - x$$

by the additive identity axiom.
Thus we have shown that *if* $a + x = b$ *then* $x = b - a$ (i.e., x *must* equal $b - a$).

3. Suppose $a + x = x + a = a$ for all a. (We want to prove from this that $x = 0$, in other words that x *must* equal 0.)

From the fact $a + x = a$, we immediately have from part 2 of the exercise that $x = a - a$ (*why?*) But $a - a = a + (-a) = 0$ (by the definition of $a - a$ for the first equality and the additive inverse axiom for the second), and so $x = 0$ as required. □

Remark.

• The first part of the question was to show that two quantities (or numbers) are equal. The above proof begins with one of these *numbers*, namely $a + (b - a)$, and by a series of equalities each of which was justified by a particular axiom, ends up with the other number, namely b.

• This is logically different from beginning with the *statement to be proved*, namely $a + (b - a) = b$, and then proceeding by a series of statements to something which is true. In fact, doing this is *not* a valid proof.

For example, many students gave a "proof" that went something like the following:

"Solution". Begin with

$$
\begin{aligned}
a + (b - a) &= b. \\
\text{Hence } a + (b + (-a)) &= b \quad \text{by the definition of } b - a \\
\text{Hence } a + ((-a) + b) &= b \quad \text{by the commutative axiom for } + \\
\text{Hence } (a + (-a)) + b &= b \quad \text{by the associative axiom for } + \\
\text{Hence } 0 + b &= b \quad \text{by the additive inverse axiom} \\
\text{Hence } b &= b \quad \text{by the additive identity axiom}
\end{aligned}
$$

Since this is true, we have "established" the rquired result. □

What has really been establised in the above argument is that *if* $a + (b - a) = b$ *then* $b = b$. Not a very interesting result, since we already know from the meaning of "=" that $b = b$!

Put alternatively, if P is the statement $a + (b - a) = b$ and Q is the statement $b = b$, then what the above "solution" really shows is that $P \Rightarrow Q$. What we want to show is that $Q \Rightarrow P$; since Q is certainly a true statement it then follows by the rules of logic that P is also true.

However (and this is the good news in this particular example) every step in the above *"Solution"* is reversible, and this leads to a valid proof as follows:

Solution.

$$
\begin{aligned}
0 + b &= b \quad \text{by the additive identity axiom} \\
\text{Hence } (a + (-a)) + b &= b \quad \text{by the additive inverse axiom} \\
\text{Hence } a + ((-a) + b) &= b \quad \text{by the associative axiom for } + \\
\text{Hence } a + (b + (-a)) &= b \quad \text{by the commutative axiom for } + \\
\text{Hence } a + (b - a) &= b \quad \text{by the definition of } b - a
\end{aligned}
$$

This completes the proof. □

It is a matter of taste, but I prefer the first proof.

• You should be aware of the fact that most arguments are *not* reversible. For example, suppose we begin with the (false) statement that

$$
\begin{gathered}
0 = 1 \\
\text{Then } 0 \times 0 = 0 \times 1 \\
\text{Hence } 0 = 0
\end{gathered}
$$

The above is a valid argument of the not very interesting fact that $0 = 1 \Rightarrow 0 = 0$. But the argument certainly cannot be "reversed" to give a proof that $0 = 0 \Rightarrow 0 = 1$, and hence that $0 = 1$ (using the extra fact that $0 = 0$ is indeed a true statement). The problem is essentially that one cannot divide by zero.

• Another common mistake was to write $a + b + c$ for various a, b, c. This can mean either $(a + b) + c$ or $a + (b + c)$, and in this type of question you should use brackets to indicate which is meant. See also the remark at the end of Exercise 2.

• Most students did not realise that part 3 of the question was an easy consequence of part 2. In the original question I wrote "deduce"; I should probably have written "hence deduce form the previous part".

• A very quick proof of part 3 is as follows:

Solution. Suppose $a+x = x+a = a$ for all a. In particular, taking $a = 0$, it follows that $x + 0 = 0$. By the additive identity axiom applied to the left side, it follows that $x = 0$. □

In the following exercises, do *not* give proofs from the axioms. Use all the usual properties of addition, multiplication, subtraction, division and inequalities, without further justification.

Exercise 5. *An exercise in clear thinking.* For each of the following statments, say if it is true or false, and give a short justification.

1. For every real number $x > 0$ there exists a real number y such that $0 < y < x$.
2. There exists a real number y such that for every real number $x > 0$, $0 < y < x$.
3. For every real number $x > 0$ and for every real number y, $0 < y < x$.
4. For every real number y and for every real number $x > 0$, $0 < y < x$.
5. There exists a real number y and there exists a real number $x > 0$ such that $0 < y < x$.
6. There exists a real number $x > 0$ and there exists a real number y such that $0 < y < x$.

Solution.
1. True. Given $x > 0$, let $y = x/2$. Then $0 < y < x$.
2. False. The statment implies there is a real nmber (y) which is greater than 0 and less than every positive real number (x). This is false, since no matter which y we might take, we get a contradiction by letting $x = y/2$ (or even by letting $x = y$).
3. False. In particular, it is certainly not true for every real number y, that $y > 0$.
4. False. This statement has the same meaning as the previous statement.
5. True. Just take $x = 2$ and $y = 1$.
6. True. This statement has the same meaning as the previous statement. □

Exercise 6.

1. Prove that for every integer $n > 0$ one has
$$n = 3m,\ 3m + 1 \text{ or } 3m + 2$$
for some integer m.
2. Prove that the square of any integer of the first kind is again of the first kind, but that the square of any integer of the second or third kind is of the second kind.
3. Prove there is no rational number $x > 0$ such that $x^2 = 3$ by a similar argument to that in Theorem 2.11 (except that now, instead of working with odd and even integers, one works with integers of the first, second, or third kind.)

Solution.

1. If n is divided by 3, the remainder will be either 0, 1 or 2. That is,

$$n = 3m,\ 3m + 1 \text{ or } 3m + 2.$$

$\Big($The above is all that was required. But in more detail, let m be the largest integer such that $3m \leq n$. Then $n - 3m = 0, 1,$ or 2; since if $n - 3m \geq 3$ then $3(m + 1) \leq n$ which contradicts the definition of m. This gives the result.$\Big)$

2. Since $(3m)^2 = 9m^2 = 3(3m^2)$, the square of an integer of the first kind is again of the first kind.

   Since $(3m + 1)^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$, the square of an integer of the second kind is of the second kind.

   Since $(3m + 2)^2 = 9m^2 + 12m + 4 = 3(3m^2 + 4m + 1) + 1$, the square of an integer of the third kind is of the second kind.

3. Suppose (in order to gain a contradiction) that x is a positive rational number for which $x^2 = 3$. This means that, after cancellation if necessary, we can write

$$x = m/n$$

where m and n are positive integers which have *no* common factors. Squaring both sides of the equation, we have

$$3 = m^2/n^2$$

and hence

$$m^2 = 3n^2.$$

It follows that m^2 is of the first kind (i.e. is divisible by 3), and so from Part 2, m is also of the first kind (as otherwise its square would be of the second kind). But since m is of the first kind, we can write

$$m = 3p$$

for some integer p, and hence

$$m^2 = 9p^2.$$

Substituting this into $m^2 = 3n^2$ gives

$$9p^2 = 3n^2,$$

and hence

$$3p^2 = n^2.$$

But now we can argue as we did before for m, and deduce that n is also of the first kind (divisible by 3). Thus m and n both have the common factor 3, which contradicts the fact they have no common factors.

This contradiction implies that our original assumption was wrong, and so x is not rational.

$\square$

Remark.

- In part 2, by saying "n is an integer of the first kind", I meant of the first kind as in part 1. In other words, $n = 3m$ for some integer m, or in other words "n is divisible by 3".

Likewise, "n is an integer of the second kind" meant of the second kind as in part 1. In other words, $n = 3m + 1$ for some integer m, or in other words "n has a remainder of 1 after being divided by 3".

Similarly for the third kind.

- The proof of the first part was essentially a matter of noting that the given conditions were equivalent to the fact that the remainder after dividing n by 3 is either 0, 1 or 2. Since this is standard, and since in this question you were asked not to work from the axioms, there was no need to say much more.
- Part 2 was just a calculation.
- This was the main point to the question. Instead of having odd and even integers as in the proof that there is no rational number x such that $x^2 = 2$, we here have to work with integers of the first, second or third kind.