2.1
Using the axioms or results, prove that \(- (a + b) = (−a) + (−b)\) for all \(a\) and \(b\).

I will show two ways to do this. First, recall that \(- (a + b)\) is the additive inverse of \(a + b\), so we only have to show that \((−a) + (−b)\) is also such an inverse. First, we note that

\[
(a + b) + ((−a) + (−b)) = (a + b) + ((−b) + (−a))
\]

by commutativity (A1). Then we use associativity (A2) to write

\[
(a + b) + ((−b) + (−a)) = a + (b + ((−b) + (−a))) = a + ((b + (−b)) + (−a)).
\]

By A4 and A3 (additive inverse and identity), this is the same as \(a + (0 + (−a)) = a + (−a) = 0\). But that means \((−a) + (−b)\) is an additive inverse to \(a + b\), so we are done.

The other way is to use the fact that \(-c = (−1)c\) for all \(c\). In that case, using distributivity and the fact we see that

\[
-(a + b) = (−1)(a + b) = (−1)a + (−1)b = (−a) + (−b).
\]

2.3a
The first operation does not satisfy cancellation, as \(b \circ a = b \circ b = c\), but \(b \neq a\). I didn’t actually assign the second one, but if you look at each row you will notice that if \(y \neq z\) along the top, then \(xy \neq xz\) in the row. For instance, in the first row, \(ay\) is different for every \(y\), so there is no such problem. So cancellation holds.

2.4(b,c,f)
Prove the following using the definitions:

- \((a - b) - (c - d) = (a + d) - (b + c)\)
- \((a - b)(c - d) = (ac + bd) - (ad + bc)\)
- \(\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}\)

We start with \((a - b) - (c - d)\). Use the definition of subtraction, and rewrite it as \((a + (−b)) + ((−c) + (−d)))\). Now we use the fact we just proved above, and write it as \((a + (−b)) + ((−c) + (−d))) = (a + (−b)) + ((−c) + d)\) (using the fact proved in class that the inverse of the inverse is just the number itself). Now we use associativity and commutativity to write

\[
(a + (−b)) + ((−c) + d) = a + ((−b) + ((−c) + d)) = a + ((−b) + (−c)) + d
\]

\[
= a + (d + ((−b) + (−c))) = (a + d) + ((−b) + (−c)).
\]

Finally, we use the fact above again and write this as \((a + d) + (−(b + c)) = (a + d) - (b + c)\), where the last step is by definition of subtraction.

We start with \((a - b)(c - d)\). Use the definition of subtraction, and get \((a + (−b)))(c + (−d))\). Now we distribute twice (or three times, depending on how you count it):

\[
a(c + (−d)) + (−b)(c + (−d)) = (ac + a(−d)) + ((−b)c + (−b)(−d)).
\]
Then we rewrite, using the fact proved in class that \(-x(y) = -xy\) and the fact used above that \(-(-x) = x\):

\[(ac + (-ad)) + ((-bc) + ((-bd))) = (ac + (-ad)) + ((-bc) + bd)\]

Now we use commutativity and associativity:

\[ac + ((-ad) + ((-bc) + bd)) = ac + ((-ad) + ((-bc) + bd)) = ac + (bd + ((-ad) + ((-bc))))\]

Finally we use the fact about subtracting two things, and the definition of subtraction again:

\[(ac + bd) + ((-ad + bc)) = (ac + bd) - (ad + bc)\]

which is what we wanted.

We start with \(\frac{a}{c} + \frac{b}{d}\). This is rewritten as \(a(b^{-1}) + c(d^{-1})\). We use the existence of the multiplicative identity 1 and rewrite it again as \(a(b^{-1})(1) + c(d^{-1})(1)\). Now we use the fact that \(b\) and \(d\) have inverses, and that \(x(x^{-1}) = 1\), and write the 1’s in an unusual way:

\[a(b^{-1})(d(d^{-1})) + c(d^{-1})(b(b^{-1}))\]

We use commutativity and associativity of multiplication a number of times:

\[a(b^{-1})(d(d^{-1})) + c(d^{-1})(b(b^{-1})) = a(b^{-1}d)(d^{-1}) + c(d^{-1}b)(b^{-1})\]

\[= a(db^{-1})(d^{-1}) + c(bd^{-1})(b^{-1}) = (ad)(b^{-1}d^{-1}) + (cb)(d^{-1}b^{-1})\]

\[= (ad)(d^{-1}b^{-1}) + (bc)(d^{-1}b^{-1})\]

Use distributivity, and get \((ad + bc)(d^{-1}b^{-1})\). Now, note that the multiplicative inverse of \(bd\) is \(d^{-1}b^{-1}\), since

\[(bd)(d^{-1}b^{-1}) = b(d(d^{-1}b^{-1})) = b(dd^{-1}(b^{-1}))\]

\[= b(1(b^{-1})) = bb^1 = 1\]

So, we can rewrite \((ad + bc)(d^{-1}b^{-1})\) as \((ad + bc)(bd)^{-1}\). But by definition of division, this is \(\frac{ad + bc}{bd}\), as desired.

2.8 For this problem, Isaac Yonemoto has given us the solutions.

1. Proofs for 2.8

1.1. Some Definitions. Remember, \(\exists\) means “there exists”, and \(\forall\) means “for all”, \(\mid\) means “such that”.

\(S\) is some set that satisfies A1-A4, M1-M3, and D.

\(Z \subseteq S\) so that \(Z = x \in S | \exists a \neq 0, x \cdot a = 0\) Note that this is equivalent to the “set of all zero divisors, and zero”. \(T \subseteq S\) so that \(T = x \in S | \forall a \neq 0, x \cdot a \neq 0\)

Convince yourself that this is “everything that is neither zero divisor nor zero”. Also convince yourself that everything that is is in \(S\) is either in \(T\) or in \(Z\), that is if \(x \notin T\) then \(x \in Z\), and vice versa.

1.2. Problem 2.8 a. I know I went over this in tutorial, but let me reiterate it to demonstrate the structure of a proof. All proofs start with an set of preconditions (or hypotheses). These are the “givens” for the proof.
Preconditions.

\( a, b \in \mathbb{Z} \)

You could argue that those definitions I put up above, were also “preconditions”, it’s only a matter of how you want to organize things. Note that this sets up the PROPOSITION, what we want to show.

Proposition.

\( a \cdot b \in \mathbb{Z} \)

Note that this the symbolic way of saying “multiplication on \( \mathbb{Z} \) is closed” – that the result stays in the set. On to the PROOF.

Proof. \( b \in \mathbb{Z} \) means that

\[ \exists c \in S \mid b \cdot c = 0 \]

Also note that the definition of \( \mathbb{Z} \) ensures that \( c \neq 0 \). Remember that, it will come up again.

By the closure of multiplication in \( S \),

\[ a \cdot (b \cdot c) = a \cdot 0 \]

We have a theorem that says \( a \cdot 0 = 0 \), so by transitivity of equality:

\[ a \cdot (b \cdot c) = 0 \]

Now use M2 to switch things around a bit:

\[ (a \cdot b) \cdot c = 0 \]

Remember, \( c \neq 0 \), so... that means that \( a \cdot b \in \mathbb{Z} \) by the definition of \( \mathbb{Z} \)!

1.3. Problem 2.8 b.

Preconditions.

\( x \in S, \exists ! x^{-1} \mid x \cdot x^{-1} = 1 \)

By \( \exists ! \), we mean there “exists a unique”... Remember, this comes straight from the definition of inverse (see M4).  

Proposition.

\( x \in T \)

Remember what it means to be in \( T \), and carefully note that it is not explicitly the same as the precondition. Also carefully note the DIRECTION of logic. We want to show that the existence of an inverse guarantees membership in \( T \). 

Proof, by contradiction. Here we prove by contradiction. Contradict the PROPOSITION and show that it leads to a fallacy.

Assume \( x \notin T \).

This means, as I asserted in the beginning, \( x \in \mathbb{Z} \). In particular,

\[ \exists a \neq 0 \mid x \cdot a = 0 \]

By the closure of multiplication in \( S \), and our precondition (which asserts the inverse of \( x \)) we then can deduce that:

\[ x^{-1} \cdot (x \cdot a) = x^{-1} \cdot 0 = 0 \]

Use M2 to change this to:

\[ (x^{-1} \cdot x) \cdot a = 0 \]
By the definition of the inverse, we then have

\[ 1 \cdot a = 0 \]

Using M3, we have:

\[ a = 0 \]

But this is a contradiction! We chose \( a \) to be precisely nonzero, which means that our assumption is faulty (thanks to the contrapositive)....

1.4. **Problem 2.8 c.** See if you can follow this proof. I won’t give reasons, you figure out what the reason for each step is.

**Preconditions.**

\( a, b \in T \)

**Proposition.**

\( a \cdot b \in T \)

**Proof, by contradiction.** Assume \( a \cdot b \in \mathbb{Z} \).

\[ \Rightarrow \exists c \neq 0 \mid (a \cdot b) \cdot c = 0 \]

\[ \Rightarrow a \cdot (b \cdot c) = 0 \]

\[ \Rightarrow a \in \mathbb{Z} \]

**Contradiction!**

2.9

Let \( S \) be a set with addition satisfying axioms A1-A4. Show that the additive identity of \( S \) is unique.

Suppose we have two numbers \( x \) and \( y \) such that for every \( s \in S \), \( x + s = s \) and \( y + s = s \) (the text hints to call them 0 and 0’). Well, that means that \( x + s = y + s \), since they both equal \( s \). But now add \(-s\) to both sides: this gives \((x + s) + (-s) = (y + s) + (-s)\), which by A2 is the same as \( x + (s + (-s)) = y + (s + (-s)) \), which by A4 is the same as \( x + 0 = y + 0 \). But by A3 this is just \( x = y \). So any two numbers which are the additive identity are the same; hence, there is only one such number, and that means it’s unique.