HOMEWORK SOLUTIONS 14/04/03

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

$$-(a+b) = (-1)(a+b) = (-1)a+(-1)b = (-a)+(-b).$$

2.4(a,c,f)

Prove the following from the definitions:

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

We start with $(a-b)+(c-d)$. Use the definition of subtraction and write it as $(a+(-b))+(c+(-d))$. Now we use associativity a couple times to write it as $a+((-b)+(c+(-d))) = a+(((-b)+c)+(-d))$. Then we use commutativity on the middle, so it's also $a+((c+(-b))+(-d))$. Now we reverse the use of associativity to write $a+(c+((-b)+(-d))) = (a+c)+((-b)+(-d))$. Now, by Theorem 2.3, we can take out -1 to make this $(a+c)+((-1)b+(-1)d)$; by distributivity this is $(a+c)+(-1)(b+d)$. Now a final use of Theorem 2.3 and the definition of subtraction yields $(a+c)+(-(b+d)) = (a+c)-(b+d)$.

Next, we start with $(a-b)(c-d)$. Use the definition of subtraction to rewrite this as $(a+(-b))(c+(-d))$. Now we use distribution, commutativity, then distribution again:

$$(a+(-b))c+(a+(-b))(-d) = c(a+(-b))+(-d)(a+(-b)) =$$
$$(ca+c(-b))+((-d)a+(-d)(-b)).$$

We use both multiplicative and additive commutativity next, namely

$$(ca+c(-b))+((-d)a+(-d)(-b)) = (ac+(-b)c)+(a(-d)+(-b)(-d)) =$$
$$(ac+(-b)c)+((-b)(-d)+a(-d)),$$

which can be further refined using A1 and A2 some more to get

$$(ac+(-b)c)+((-b)(-d)+a(-d)) = ac+((-b)c+((-b)(-d)+a(-d))) =$$

$$ac + (((-b)c + (-b)(-d)) + a(-d)) = ac + (((-b)(-d) + (-b)c) + a(-d)) =$$

$$ac + ((-b)(-d) + ((-b)c + a(-d))) = (ac + (-b)(-d)) + ((-b)c + a(-d)).$$

Next, we use Theorem 2.4 and Practice Problem 2.2 to write this as $(ac + bd) + (-bc + (-ad))$. Then we once again use Theorem 2.3 and distributivity to write $(ac + bd) + ((-1)bc + (-1)ad) = (ac + bd) + (-1)(bc + ad)$. Finally, use Theorem 2.3, the definition of subtraction, and A1 yet again to get your desired result.

Finally, we examine division. $\frac{a}{b} + \frac{c}{d}$ is defined to be $ab^{-1} + cd^{-1}$. We can multiply both terms by 1 in the forms dd^{-1} and bb^{-1}, respectively; the fact that 1 takes these forms is M4, and the fact we can multiply is M3. So we end up with $(ab^{-1})(dd^{-1}) + (cd^{-1})(bb^{-1})$. Hopefully by now you can fill in the details of associativity and commutativity to end up with $(ad)(b^{-1}d^{-1}) + (bc)(b^{-1}d^{-1})$. Using commutativity, distributivity, and commutativity again, this yields $(ad + bc)(b^{-1}d^{-1})$. However, we note that $b^{-1}d^{-1} = (bd)^{-1}$; this is proved by observing that $(bd)(b^{-1}d^{-1}) = (bb^{-1})(dd^{-1}) = 1 \cdot 1 = 1$ (using M2 and M1 several times, then M4 and M3), so that $b^{-1}d^{-1}$ is a multiplicative inverse for $(bd)^{-1}$. Hence our expression $(ad+bc)(b^{-1}d^{-1})$ may be written $(ad+bc)(bd)^{-1}$, which by the definition of division is $\frac{ad+bc}{bd}$, as desired.

2.8(a,b)

Suppose S is as in the book. We are letting $Z = \{0\} \cup \{$ zero-divisors $\}$. We will prove Z is closed under multiplication, and that if $x \in S$ has a multiplicative inverse, then $x \in T$.

First, we show closure of Z. Let $a, b \in Z$. If either a or b is zero, then certainly $ab = 0$, so in this case $ab \in Z$. If neither a nor b is zero, then still if $ab = 0$ we are done. Assume that neither a nor b is zero, and even that $ab \neq 0$. We know (since a is in Z) that there is some number $c \neq 0$ such that $ac = 0$, by definition of zero-divisor. If I can show $(ab)c = 0$, then I have shown that ab is in Z. However, this is easy; $(ab)c = (ba)c = b(ac) = b(0) = 0$. This uses, in order, M1, M2, the assumption that $ac = 0$, and Theorem 2.2.

Now assume that x has a multiplicative inverse y, such that $xy = 1$. If we can show that the only a such that the product $ax = 0$ is $a = 0$, then we have shown that $a \notin Z$, so $a \in T$. So assume $ax = 0$. Then multiply both sides by y. That gives $(ax)y = 0y$. We use M2 on the left hand side and M1 on the right hand side to get $a(xy) = y(0)$. By Theorem 2.2, the right hand side is zero; by assumption, $xy = 1$. Thus, $a(1) = 0$. But by M3, $a(1) = a$, so $a = 0$, which was my claim. So I'm done.

2.9

We assume S is an Abelian group under addition. Then we wish to show that if $a + 0 = 0 + a = a$ and $a + 0' = 0' + a = a$ for every a, then $0 = 0'$. The easiest way to do this is to note that all four things equal a. Thus, $0 + a = 0' + a$. But then we can use Theorem 2.1 to cancel a, so $0 = 0'$ as desired.

2.11

Let $<$ be the ordinary order on $\mathbb{R}$. Prove that if $0 < a < b$ and $0 < c < d$, then $ac < bd$. Also prove that if $n = ab$, and all three are positive, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Since $c > 0$ and $a < b$, we can use O4 to say that $ac < bc$. Since $b > 0$ and $c < d$, by the same axiom we can write $cb < db$. Now multiplication on the reals is commutative (M1), so that is the same as $bc < bd$. But by transitivity (O3) that means $ac < bd$.

For the second part, let's assume the opposite - that both a and $b > \sqrt{n}$. Then $a > \sqrt{n} > 0$ and $b > \sqrt{n} > 0$. By the first part, this means $ab > (\sqrt{n})^2$. But $(\sqrt{n})^2 = n$. Hence $ab > n$, which is a contradiction. Thus our assumption wasn't true; so at least one of a or b is less than or equal to $\sqrt{n}$.

2.12(a,c)

Suppose we have an order satisfying axioms O1-O4. Prove, for a, b, x, y in the set, that if $a - x < a - y$ then $x > y$, and that if $0 < a < b$ then $a^2 < b^2$.

Assume $a - x < a - y$. This may be written $a + (-x) < a + (-y)$ by definition of subtraction, and $(-x) + a < (-y) + a$ by commutativity (A1). Now add $-a$ to both sides (allowed by axiom O3), which gives $((-x) + a) + (-a) < ((-y) + a) + (-a)$. Use associativity (A2) to write this as $(-x) + (a + (-a)) < (-y) + (a + (-a))$. Then A4 says $(a + (-a)) = 0$, so $(-x) + 0 < (-y) + 0$ and hence $-x < -y$ by A3 (additive identity). Finally, Theorem 2.8 says that $-(-x) > -(-y)$; but since $-z + z = 0$ for any z, clearly the additive identity $-(-z)$ of $-z$ is just z, so this says $x > y$ as desired.

Assume $0 < a < b$. Since $b > 0$ and $a < b$, we can use O4 to write $ab < b^2$; similarly, since $a > 0$, we can write $a^2 < ba$. Use A1 to rewrite this as $a^2 < ab$; then transitivity (O3) gives that $a^2 < b^2$. We could also have used exercise 2.11 if it had been in the text.

2.15

The set of odd natural numbers certainly has a least element; it is 1. The set of positive rational numbers does not; if you have a potential smallest number $\frac{a}{b}$, note that this is greater than or equal to $\frac{1}{b}$. But this is greater than $\frac{1}{b+1}$, which is a smaller rational number. So you can always get a smaller positive rational number. Part c) is identical to part b). As for the set of rational numbers greater than π, this also does not have a least element. It is more tricky to see; the basic idea is that once you show that *every* positive number is greater than $\frac{1}{n}$ for some (big) $n \in \mathbb{N}$, taking a number x bigger than π leads us to look at $x - \pi > \frac{1}{n}$ (for some n), and we use the same trick, but more carefully to ensure getting a rational number. And as I mentioned in class, any finite set of numbers has a least element, just by comparing them all with each other in finite time.