

ABSTRACT ALGEBRA A
HOMEWORK 2 SOLUTIONS

2-4. I thought this was going to be a tricky double or triple induction, but it turns out just to be a simple induction on c .

First, we show that addition is associative when $c = 1$. The definition of addition says that

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

Here the first and last equalities are from the base case of the definition of addition, and the middle equality is from the inductive part of the definition.

Now suppose that $a + (b + c) = (a + b) + c$, and try to show associativity holds for $s(c)$ as well. We get

$$a + (b + s(c)) = a + s(b + c) = s(a + (b + c)) = s((a + b) + c) = (a + b) + s(c).$$

This time, the first and fourth equalities are from the base case definition of addition; the second equality is from the inductive case of the definition, and the third equality is from the induction hypothesis.

With our definition of \mathbb{N} as starting at 1, \mathbb{N} lacks both an identity element and inverses.

2-9. To show that \sim is reflexive, we have to show that for every x and y in \mathbb{N} , $(x, y) \sim (x, y)$. That is, we have to show that $x + y = y + x$, which we're assuming we know.

For symmetry, we have to show that if $(x, y) \sim (z, w)$, then $(z, w) \sim (x, y)$. That is, we have to show that if $x + w = y + z$, then $z + y = w + x$. Again, this follows from commutativity of addition in \mathbb{N} .

Finally, for transitivity, we start out by assuming that $(x, y) \sim (z, w)$ and that $(z, w) \sim (s, t)$, that is, that $x + w = y + z$ and that $z + t = w + s$. We have to prove that $(x, y) \sim (s, t)$, i.e., that $x + t = y + s$. We do this by adding the two equations we are given, to get

$$(x + w) + (z + t) = (y + z) + (w + s).$$

A small blizzard of commutativity and associativity transforms this into

$$(x + t) + (w + z) = (y + s) + (w + z).$$

Cancellation then gives us $x + t = y + s$, as desired.

2-15. Oh, how about $(8, 2)$ and $(400, 100)$ and $(-68, -17)$, and $(1492, 373)$?

2-16. This is a lot like Problem 2-9. Just replace all the additions with multiplications.

2-18. $(7/8) + (-5/12) = (7, 8) + (-5, 12) = (7 \cdot 12 + 8(-5), 8 \cdot 12) = (44, 96) = 44/96$. A sum of equivalent pairs would be

$$\frac{21}{24} + \frac{-50}{120} = \frac{(21)(120) + (24)(-50)}{(24)(120)} = \frac{1320}{2880}.$$

Notice that $(44, 96) \sim (1320, 2880)$.

Multiplication works the same way, but simpler.

2-19. To show this, we have to show that $(a, b) \sim (an, bn)$, i.e., that $a(bn) = b(an)$. This is an immediate consequence of the commutativity and associativity of multiplication in \mathbb{Z} .

2-20. We have to show that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \sim \frac{(an)d + (bn)c}{(bn)d} = \frac{an}{bn} + \frac{c}{d}.$$

In other words, we have to show that

$$(ad + bc)((bn)d) = (bd)((an)d + (bn)c).$$

This is just a matter of lots of commutativity and associativity in \mathbb{Z} .

2-21. We have to show that

$$\frac{a}{b} \frac{c}{d} = \frac{ac}{bd} \sim \frac{(an)c}{(bn)d} = \frac{an}{bn} \frac{c}{d},$$

i.e., that $(ac)((bn)d) = (bd)((an)c)$. As usual, this is just associativity and commutativity of multiplication in \mathbb{Z} .

2-22. I'll actually do a bit more than the problem demands. I'll start out by proving carefully that addition is well-defined in \mathbb{Q} . What we need to show is that if $\langle(a, b)\rangle = \langle(a', b')\rangle$ and if $\langle(c, d)\rangle = \langle(c', d')\rangle$, then

$$\langle(a, b)\rangle + \langle(c, d)\rangle = \langle(a', b')\rangle + \langle(c', d')\rangle.$$

In other words, we are assuming that $(a, b) \sim (a', b')$ and that $(c, d) \sim (c', d')$, and we are attempting to prove that

$$(ad + bc, bd) \sim (a'd' + b'c', b'd').$$

Taking apart the definition of equivalence, we are assuming that $ab' = ba'$ and that $cd' = dc'$, and we are attempting to prove that

$$(ad + bc)(b'd') = (bd)(a'd' + b'c').$$

This is easy, though:

$$\begin{aligned} (ad + bc)(b'd') &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (dc')(bb') \\ &= (bd)(a'd' + b'c'). \end{aligned}$$

Let me now prove commutativity of addition, because that will be convenient to have when we do the rest of the problem. It's also a one-liner:

$$\langle(a, b)\rangle + \langle(c, d)\rangle = \langle(ad + bc, bd)\rangle = \langle(cb + da, db)\rangle = \langle(c, d)\rangle + \langle(a, b)\rangle.$$

The middle equality here follows from the commutativity of addition and multiplication in \mathbb{Z} ; the other equalities are just the definition of addition in \mathbb{Q} .

Now I claim that $\frac{0}{1} = \langle(0, 1)\rangle$ is an identity element for addition. Again, this is easy:

$$\langle(0, 1)\rangle + \langle(a, b)\rangle = \langle(0b + 1a, 1b)\rangle = \langle(a, b)\rangle$$

shows that $\frac{0}{1}$ is a left identity, and commutativity does the rest of the job.

Finally, I claim that $\langle(-a, b)\rangle$ is an inverse for $\langle(a, b)\rangle$. When we add these, we get

$$\langle(a, b)\rangle + \langle(-a, b)\rangle = \langle(ab + b(-a), bb)\rangle = \langle(0, bb)\rangle,$$

using the fact that we know everything about the arithmetic of \mathbb{Z} . But now $01 = (bb)0$; so $(0, bb) \sim (0, 1)$; so $\langle(0, bb)\rangle = \langle(0, 1)\rangle$; so $\langle(-a, b)\rangle$ is a right inverse of $\langle(a, b)\rangle$. Commutativity shows that it is also a left inverse, and we're done.

2-23. Let me again write this using our language of equivalence classes. First of all, if $\langle(a, b)\rangle$ and $\langle(c, d)\rangle$ are elements of \mathbb{Q} , then $b \neq 0$ and $d \neq 0$; so $bd \neq 0$; so

$$\langle(a, b)\rangle\langle(c, d)\rangle = \langle(ac, bd)\rangle \in \mathbb{Q}.$$

Now we have to show that multiplication is well-defined, that is that if $\langle(a, b)\rangle = \langle(a', b')\rangle$ and if $\langle(c, d)\rangle = \langle(c', d')\rangle$, then $\langle(a, b)\rangle\langle(c, d)\rangle = \langle(a', b')\rangle\langle(c', d')\rangle$.

So we assume that $(a, b) \sim (a', b')$ and that $(c, d) \sim (c', d')$, and we want to prove that $(ac, bd) \sim (a'c', b'd')$.

In other words, we assume that $ab' = ba'$ and that $cd' = dc'$, and we want to prove that $(ac)(b'd') = (bd)(a'c')$. This is easy:

$$(ac)(b'd') = (ab')(cd') = (ba')(dc') = (bd)(a'c'),$$

and we're done.

2-24. This one turns out to be a straightforward computation:

$$\begin{aligned} \langle(a, b)\rangle\langle(c, d)\rangle\langle(e, f)\rangle &= \langle(ac, bd)\rangle\langle(e, f)\rangle \\ &= \langle((ac)e, (bd)f)\rangle \\ &= \langle(a(ce), b(df))\rangle \\ &= \langle(a, b)\rangle\langle(ce, df)\rangle \\ &= \langle(a, b)\rangle\langle(c, d)\rangle\langle(e, f)\rangle. \end{aligned}$$

2-25. As in Problem 2-22, let's start with commutativity. It's easy:

$$\langle(a, b)\rangle\langle(c, d)\rangle = \langle(ac, bd)\rangle = \langle(ca, db)\rangle = \langle(c, d)\rangle\langle(a, b)\rangle,$$

because of the definition of multiplication in \mathbb{Q} and the commutativity of multiplication in \mathbb{Z} .

Next, $\langle(1, 1)\rangle$ is a left identity because for any $\langle(a, b)\rangle \in \mathbb{Q}$, we have

$$\langle(1, 1)\rangle\langle(a, b)\rangle = \langle(1a, 1b)\rangle = \langle(a, b)\rangle.$$

It's also a right identity by commutativity.

Now let $\langle(a, b)\rangle \in \mathbb{Q}$, $\langle(a, b)\rangle \neq 0$. Then $a \neq 0$. (Why? Because if $a = 0$, then $a1 = 0 = b0$; so $(a, b) \sim (0, 1)$; so $\langle(a, b)\rangle = \langle(0, 1)\rangle = 0 \in \mathbb{Q}$.) This means that $\langle(b, a)\rangle \in \mathbb{Q}$; and

$$\langle(a, b)\rangle\langle(b, a)\rangle = \langle(ab, ba)\rangle.$$

But $(ab)1 = (ba)1$; so $(ab, ba) \sim (1, 1)$; so $\langle(ab, ba)\rangle = \langle(1, 1)\rangle = 1 \in \mathbb{Q}$; so $\langle(b, a)\rangle$ is a right inverse of $\langle(a, b)\rangle$. By commutativity, it is also a left inverse.

Finally, distributivity is just an unpleasant computation:

$$\begin{aligned} \langle(a, b)\rangle(\langle(c, d)\rangle + \langle(e, f)\rangle) &= \langle(a, b)\rangle\langle(cf + de, df)\rangle \\ &= \langle(a(cf + de), b(df))\rangle. \end{aligned}$$

Similarly,

$$\begin{aligned} \langle(a, b)\rangle\langle(c, d)\rangle + \langle(a, b)\rangle\langle(e, f)\rangle &= \langle(ac, bd)\rangle + \langle(ae, bf)\rangle \\ &= \langle((ac)(bf) + (bd)(ae), (bd)(bf))\rangle. \end{aligned}$$

To show that these are equal, we must show that

$$\langle (a(cf + de), b(df)) \rangle \sim \langle ((ac)(bf) + (bd)(ae), (bd)(bf)) \rangle,$$

i.e., that

$$[a(cf + de)][(bd)(bf)] = [b(df)][(ac)(bf) + (bd)(ae)].$$

This is easy, because multiplying out either side gives $ab^2cdf^2 + ab^2d^2ef$.

2-27. The natural way to do this is probably to define a mapping $\phi : \mathbb{Z} \rightarrow \mathbb{Q}_2$ by $\phi(n) = n/2$. In proving that this is an isomorphism, I'll assume we know everything about the arithmetic of \mathbb{Q} , so that I don't have to keep playing the games above.

First of all, it's obvious that ϕ is surjective, since any element of \mathbb{Q}_2 can be written in the form $n/2 = \phi(n)$. It's equally obvious that ϕ is injective, since

$$\phi(n) = \phi(m) \implies \frac{n}{2} = \frac{m}{2} \implies n = m.$$

It's also not hard to show that ϕ is a homomorphism:

$$\phi(n + m) = \frac{n + m}{2} = \frac{n}{2} + \frac{m}{2} = \phi(n) + \phi(m).$$

ADDITIONAL PROBLEMS

1. The group table for U_8 looks like

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

and the group table for U_{10} looks like

·	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

These groups are not isomorphic to one another, because every element in U_8 is its own inverse, and not every element in U_{10} is its own inverse. The group U_8 is isomorphic to the 4-group K_4 ; in fact, you can take 3, 5, and 7 to a , b , and c in any order and end up with an isomorphism. The group U_{10} is isomorphic to $(\mathbb{Z}_4, +)$ with the isomorphism that takes $(1, 3, 7, 9)$ to $(0, 1, 3, 2)$, resp. In the language that we have now learned, both U_{10} and \mathbb{Z}_4 are cyclic groups, having generators 3 and 1, resp.

2. The group table for U_7 looks like

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

and the group table for U_9 looks like

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

A bit of experimentation shows that U_7 is cyclic with a generator of 3, and that U_9 is cyclic with a generator of 2. The mapping that takes the powers of 3 in U_7 , $(1, 3, 2, 6, 4, 5)$ to the powers of 2 in U_9 , $(1, 2, 4, 8, 7, 5)$, is therefore an isomorphism between the two groups. They are both isomorphic to $(\mathbb{Z}_6, +)$, the isomorphisms being the maps that take these powers to $(0, 1, 2, 3, 4, 5)$, resp. Neither of these groups is isomorphic to the other group of 6 elements we have seen, D_3 , because D_3 contains no elements of order 6—it isn't cyclic.