Kris Harper
MATH 20700
October 13, 2008

Homework 2

Problem 1. *1) What is the negation of "$P(b)$, for all $b \in B$"? What about the negation of "$P(b)$, for some $b \in B$"?*
2) State $\overline{2}$ and $\overline{3}$ for the equivalence relation axioms (non-symmetry and non-transitivity). How is non-symmetry different from antisymmetry?
3) Show that the axioms for an equivalence relation are completely independent.

1) The negation of "$P(b)$, for all $b \in B$" is "$\overline{P}(b)$ for some $b \in B$". The negation of "$P(b)$ for some $b \in B$" is "$\overline{P}(b)$ for all $b \in B$."

2) Non-symmetry is stated as, "there exists $a, b \in A$ such that $a \sim b$ but $b \nsim a$." Non-transitivity is stated as "there exists $a, b, c \in A$ such that if $a \sim b$ and $b \sim c$ then $a \nsim c$." Antisymmetry is stated as "for all $a, b \in A$, if $a \sim b$ and $b \sim a$ then $a = b$."

3)

Proof. The following relations on the set $\{a, b, c\}$ satisfy each of the axioms they are assigned to:

$\{1, 2, 3\}$: $\{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$

$\{\overline{1}, 2, 3\}$: $\{(b, b), (c, c)\}$

$\{1, \overline{2}, 3\}$: $\{(a, a), (b, b), (c, c), (a, b), (c, a), (c, b)\}$

$\{1, 2, \overline{3}\}$: $\{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}$

$\{\overline{1}, \overline{2}, 3\}$: $\{(b, b), (c, c), (a, b), (c, a), (c, b)\}$

$\{\overline{1}, 2, \overline{3}\}$: $\{(b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}$

$\{1, \overline{2}, \overline{3}\}$: $\{(a, a), (b, b), (c, c), (a, b), (b, c)\}$

$\{\overline{1}, \overline{2}, \overline{3}\}$: $\{(b, b), (c, c), (a, b), (b, c)\}$ □

**** Problem 1.** *Show that the group axioms are completely independent.*

Let $(G, \circ)$ be a group where $G = \{a, b, c\}$. Enumerate the group axioms as follows:

1) $\circ$ is associative.

2) There exists an identity element in G.

3) G is solvable.

The following multiplication tables show how $\circ$ works on G such that the respective axioms are satisfied. When composing two elements the left element is taken from the vertical column and the right element is taken from the horizontal column.

$\{1,2,3\}$:

$\times$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\{\overline{1},2,3\}$:

$\times$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

$\{1,2,\overline{3}\}$:

$\times$	a	b	c
a	a	b	c
b	b	c	b
c	c	b	c

$\{\overline{1},\overline{2},3\}$:

$\times$	a	b	c
a	b	b	b
b	c	c	c
c	a	a	a

$\{\overline{1},2,\overline{3}\}$:

$\times$	a	b	c
a	a	b	c
b	b	c	a
c	b	a	b

$\{1,\overline{2},\overline{3}\}$:

$\times$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\{\overline{1},\overline{2},\overline{3}\}$:

$\times$	a	b	c
a	a	c	c
b	c	c	a
c	c	a	b

The set of axioms $\{1,\overline{2},3\}$ is satisfied by the natural numbers under addition.

** **Problem 2.** *For a ring, R, with $a,b,c \in R$ show*
1) If $a+b=a+c$ then $b=c$.
2) $a \cdot 0 = 0 \cdot a = 0$.

Proof. 1) Let $a+b=a+c$. Add the additive inverse of a to both sides so that we have

$$b = 0+b = ((-a)+a)+b = (-a)+(a+b) = (-a)+(a+c) = ((-a)+a)+c = 0+c = c.$$

2) Note that 0 is the additive identity, so $0+0=0$. Then multiply both sides by a so we have $a\cdot(0+0) = a\cdot 0$ and distributing we have $a\cdot 0 + a\cdot 0 = a \cdot 0$. Now add the additive inverse of $a \cdot 0$ to both sides so we have

$$a\cdot 0 = 0 + a\cdot 0 = (-(a\cdot 0)+a\cdot 0)+a\cdot 0 = -(a\cdot 0)+(a\cdot 0+a\cdot 0) = -(a\cdot 0)+a\cdot 0 = 0.$$

□

** **Problem 3.** *Let R be a commutative ring with 1. Show that $(R[x],+,\cdot)$ is a commutative ring with 1.*

Proof. Let $(a_n),(b_n),(c_n) \in R[x]$. Then we have

$$(a_n)+((b_n)+(c_n)) = (a_n)+(b_n+c_n) = (a_n+(b_n+c_n)) = ((a_n+b_n)+c_n) = (a_n+b_n)+(c_n) = ((a_n)+(b_n))+(c_n)$$

so $R[x]$ is associative under addition. Also

$$(a_n)+(b_n) = (a_n+b_n) = (b_n+a_n) = (b_n)+(a_n)$$

so $R[x]$ is commutative under addition. If we let $(0_n) = (d_n)$ such that $d_n = 0$ for all n, then we have

$$(0_n)+(a_n) = (0_n+a_n) = (a_n)$$

for all $(a_n) \in R[x]$. Thus (0_n) is the additive identity of $R[x]$. Then we see that for $(a_n),(b_n) \in R[x]$ we have

$$(b_n-a_n)+(a_n) = (b_n-a_n+a_n) = (b_n)$$

so $R[x]$ is solvable. Hence $(R[x], +)$ is an abelian group. Now we consider multiplication in $R[x]$. For $(a_n), (b_n), (c_n) \in R[x]$ we have

$$\begin{aligned}
(a_n) \cdot ((b_n) \cdot (c_n)) &= (a_n) \cdot \left(\left(\sum_{i=0}^{n} b_i c_{n-i} \right)_n \right) \\
&= \left(\left(\sum_{j=0}^{n} a_j \sum_{i=0}^{n-j} b_i c_{n-i} \right)_n \right) \\
&= \left(\left(\sum_{j=0}^{n} \sum_{i=0}^{n-j} a_j b_i c_{n-i} \right)_n \right) \\
&= \left(\left(\sum_{j=0}^{n} a_j b_{n-j} \sum_{i=0}^{n} c_i \right)_n \right) \\
&= \left(\left(\sum_{j=0}^{n} a_j b_{n-j} \right)_n \right) \cdot (c_n) \\
&= ((a_n) \cdot (b_n)) \cdot (c_n)
\end{aligned}$$

so $R[x]$ is associative under addition. Consider

$$(a_n) \cdot (b_n) = \left(\left(\sum_{i=0}^{n} a_i b_{n-i} \right)_n \right) = \left(\left(\sum_{i=0}^{n} a_{n-i} b_i \right)_n \right) = \left(\left(\sum_{i=0}^{n} b_i a_{n-i} \right)_n \right) = (b_n) \cdot (a_n)$$

which shows $R[x]$ is commutative under multiplication. Let (1_n) be the sequence for which $1_0 = 1$ and $1_n = 0$ for all $n \neq 0$. Then for all $(a_n) \in R[x]$ we have

$$(a_n) \cdot (1_n) = \left(\left(\sum_{i=0}^{n} a_n b_{n-i} \right)_n \right) = (a_n \cdot 1) = (a_n)$$

which means that (1_n) is the identity for $R[x]$. Finally for $(a_n), (b_n), (c_n) \in R[x]$ we have

$$\begin{aligned}
(a_n) \cdot ((b_n) + (c_n)) &= (a_n) \cdot (b_n + c_n) \\
&= \left(\left(\sum_{i=0}^{n} a_n (b_{n-i} + c_{n-i}) \right)_n \right) \\
&= \left(\left(\sum_{i=0}^{n} a_n b_{n-i} \right)_n \right) + \left(\left(\sum_{j=0}^{n} a_j c_{n-j} \right)_n \right) \\
&= (a_n) \cdot (b_n) + (a_n) \cdot (c_n)
\end{aligned}$$

which means that $R[x]$ is distributive. Since it fulfills all the axioms, $(R[x], +, \cdot)$ is a commutative ring with 1. $\square$

**** Problem 4.** *What are the zero-divisors in $R[x]$?*

Let $(a_n)(b_n) \in R[x]$ such that $(a_n) \cdot (b_n) = 0$ and $(a_n), (b_n) \neq (0_n)$. Then we can say that the first and last nonzero terms in (a_n) and (b_n) are zero divisors in R. This occurs because these terms will multiply and have no other terms of that degree in $(a_n) \cdot (b_n)$. That is, the highest and lowest nonzero index of $(a_n) \cdot (b_n)$ will be the product of zero divisors.

Lemma 1. *In a commutative ring with* 1*, for all* a *we have* $(-1) \cdot a = -a$.

Proof. Note that

$$0 = a \cdot 0 = a \cdot (1 + (-1)) = a \cdot 1 + a \cdot (-1) = a + a \cdot (-1)$$

and adding $-a$ to both sides results in $-a = a \cdot (-1)$. $\square$

**** Problem 5.** *Let* R *be an ordered commutative ring with* 1*. Show that* R *is an integral domain.*

Proof. Let $a, b, c \in R$ such that $a \neq 0$ and $ab = ac$. Then adding $-(ac)$ to both sides we have $ab + -(ac) = 0$. Using associativity, distributivity and Lemma 1 we have $a \cdot (b + (-c)) = 0$. Note also that from Lemma 1 we know that $-(b + (-c)) = ((-b) + c)$. Assuming that this quantity is not 0, there are four cases which follow from the ordering of R.

Case 1: Let $a > 0$ and $(b + (-c)) > 0$. Then $a \cdot (b + (-c)) > 0$, which is not true.

Case 2: Let $a < 0$ and $(b + (-c)) > 0$. Then from ** Problem 6 part 1) we know $-a > 0$ and so $-a \cdot (b + (-c)) > 0$. From Lemma 1 and ** Problem 6 part 1) it follows that $a \cdot (b + (-c)) < 0$ which is not true.

Case 3: Let $a > 0$ and $(b + (-c)) < 0$. This case is similar to Case 2.

Case 4: Let $a < 0$ and $(b + (-c)) < 0$. It follows from ** Problem 6 part 4) that $a \cdot (b + (-c)) > 0$ which is not true.

Since all four of the possible cases are not possible, it must be the case that $b + (-c) = 0$. Then adding c to both sides results in $b = c$. Hence, R is an integral domain. $\square$

**** Problem 6.** *Let* R *be an ordered commutative ring with* 1 *with* $a, b, c \in R$*. Show the following:*
1) $a < 0$ *if and only if* $-a > 0$.
2) $a > 0$ *if and only if* $-a < 0$.
3) If $a < b$ *and* $c < 0$ *then* $a \cdot c > b \cdot c$.
4) If $a < 0$ *and* $b < 0$ *then* $a \cdot b > 0$.
5) If $a \neq 0$*, then* $a^2 > 0$.
6) $0 < 1$.

Proof. 1) Let $a < 0$. Then add $(-a)$ to both sides. We have $0 = (-a) + a < 0 + (-a) = -a$. Similarly, assume $-a > 0$ and add a to both sides. Then $0 = a + (-a) > a + 0 = a$.
2) Assume $a > 0$. Then add $(-a)$ to both sides. We have $0 = (-a) + a > (-a) + 0 = -a$. Similarly, assume $-a < 0$ and add a to both sides. Then $0 = a + (-a) < a + 0 = a$.

3) Let $a < b$ and $c < 0$. Then $(-c) > 0$. Thus $a \cdot (-c) < b \cdot (-c)$. Add $-(a \cdot (-c))$ to both sides so we have $0 < b \cdot (-c) + (-(a \cdot (-c))$. Using associativity, commutativity, distributivity and Lemma 1 we have $0 < -((b \cdot c) + (-(a \cdot c)))$. Then $0 > (b \cdot c) + (-(a \cdot c))$ and adding $a \cdot c$ to both sides we have $a \cdot c > b \cdot c$.

4) Let $a < 0$ and $b < 0$. Then $-a > 0$ so $-(a \cdot b) = (-a) \cdot b < (-a) \cdot 0 = 0$ and $a \cdot b > 0$.

5) Let $a \neq 0$. Then either $a > 0$ or $a < 0$. Assume first that $a > 0$. Then

$$a^2 = a \cdot a > a \cdot 0 = 0.$$

If $a < 0$ then $a \cdot a > 0$ by 4).

6) We know 1 is the multiplicative identity, so $1 \cdot 1 = 1$. But then $1 = 1^2 > 0$ by 5). $\square$

Problem 2. *For an ordered integral domain* $(R, +, \cdot)$ *let* S *be an inductive subset of* R *if* $1 \in S$ *and for all* $x \in S$, $x + 1 \in S$. *Then let* N *be the intersection of all inductive subsets of* R. *Show the following: 1) Suppose that* S *is a non-empty subset of* N *such that* $1 \in S$ *and if* $x \in S$ *then* $x + 1 \in S$. *Show that* $S = N$.
2) Show that N *is closed under addition.*
3) Show that N *is closed under multiplication.*
4) Show that the well ordering principle holds in N.
5) Show that $Z = N \cup \{0\} \cup -N$ *is closed under addition.*
6) Show that Z *is closed under multiplication.*
7) Show that Z *and* $\mathbb{Z}$ *are order isomorphic.*

Proof. 1) By definition $S \subset N$. Also note that $1 \in S$ and $1 \in N$. Suppose that for some $n \in N$, $n \in S$. Then note that $n + 1$ is in both N and S so by induction, $N = S$.

2) Let $n \in N$. Let $S = \{m \in N \mid m + n \in N\}$. Note that $1 \in S$. Suppose $m \in S$. Then $m + n \in N$ and $m + n + 1 \in S$. By induction, N is closed under addition.

3) Let $n \in N$ and let $S = \{m \in N \mid mn \in N\}$. Then $1 \in S$. Suppose that $m \in S$, then $n(m + 1) = mn + m$ and $mn \in N$ and N is closed under addition so $mn + m \in N$. Thus $m + 1 \in S$ so $S = N$. Thus N is closed under multiplication.

4) Clearly a subset of N with 1 element is well ordered. Assume all subsets $S \subseteq N$ with n elements are well ordered. Consider a subset $S' \subseteq N$ with $n + 1$ elements. Let $x \in S'$ and consider $S' \backslash \{x\}$. This set is well ordered so it has a least element, y. There are then two cases, $x < y$ in which case x is the least element of S' or $x > y$ in which case y is the least element of S'. We see then that S' is well ordered. By induction, well ordering holds in N.

5) We already know that N is closed under addition and thus $-N$ is closed under addition. Addition $\{0\}$ won't change anything since it's the additive identity. Thus, the only thing we need to check is whether for $n \in N$ and $m \in -N$ we have $n + m \in Z$. Fix $n \in N$ and let S be the set of $m \in N$ such that $-m + n \in Z$. We see that $n + -1 \in Z$ so $1 \in S$. Let $m \in S$. Then using Lemma 1, associativity and distributivity

$$n + -(m + 1) = n + (-m + -1) = (n + -m) + -1$$

and $(n + -m) + -1 \in Z$. Thus the statement must hold true for all m.

6) We know that N is closed under multiplication and using ** Problem 6 we know that for $n, m \in -N$, $mn \in N$. Also, $0 \cdot n = 0$ for all n so again we must consider the product of m and n where $n \in N$ and $m \in -N$. Let $n, m \in N$ and consider $n(-m)$. Using Lemma 1 and associativity this is just $-(nm)$ which is in $-N \subseteq Z$. Thus Z is closed under multiplication.

7) Note that for all $n \in N$, we have $n \in \mathbb{Z}$. To show this, note that $1 \in \mathbb{Z}$. Then for all $n \in N$ such that $n \in \mathbb{Z}$, we have $n + 1 \in \mathbb{Z}$. Since for all $n \in \mathbb{Z}$, $-n \in \mathbb{Z}$ as well, we have $-N \subseteq \mathbb{Z}$. Then let $f : Z \to \mathbb{Z}$ be the identity function such that

$$f(n) = \begin{cases} n & \text{if } n \in N \\ 0 & \text{if } n = 0 \\ n & \text{if } n \in -N. \end{cases}$$

Then for $n, m \in Z$ we have $f(n + m) = n + m = f(n) + f(m)$ and $f(nm) = nm = f(n)f(m)$. Finally, if $n < m$ then $f(n) = n < m = f(m)$. □

**** Problem 7.** *Show that addition and multiplication on* $\mathbb{N}$ *satisfy associativity, commutativity and distributivity.*

Associative Law of Addition

Proof. Fix a and b and let S be the set of natural numbers for which the associative law holds. Then

$$(a+b)+1=(a+b)'=a+b'=a+(b+1)$$

so $1\in S$. Suppose that $c\in S$. Then $(a+b)+c=a+(b+c)$, and

$$(a+b)+c'=((a+b)+c)'=(a+(b+c))'=a+(b+c)'=a+(b+c')$$

so $c'\in S$. Thus the law holds for all natural numbers. $\square$

Commutative Law of Addition

Proof. Fix b and let S be the set of all $a\in\mathbb{N}$ for which the law holds. We have

$$b+1=1+b=b'$$

so that $1\in S$. Let $a\in S$. Then $a+b=b+a$. Thus

$$(a+b)'=(b+a)'=b+a'.$$

But also, $a'+b=(a+b)'$ by the definition of addition. Thus $a'\in S$ and the law holds for all a. $\square$

Commutative Law of Multiplication

Proof. Fix b and let S be the set of all a for which the law holds. We have $b\cdot 1=b$ and $1\cdot b=b$. Thus $1\in S$. Let $a\in S$. Then $ab=ba$. Note that

$$ab+b=ba+b=ba'$$

and by the definition of multiplication we have $a'b=ab+b$ so that $a'b=ba'$ and $a'\in S$. Thus the law holds for all a. $\square$

Distributive Law

Proof. Fix a and b and let S be the set of all c for which the law holds. We have

$$a(b+1)=ab'=ab+a=ab+a\cdot 1$$

so $1\in S$. Let $c\in S$. Then $a(b+c)=ab+ac$. Thus

$$a(b+c')=a(b+c)'=a(b+c)+a=(ab+ac)+a=ab+(ac+a)=ab+ac'$$

so that $c\in S$. Thus the law holds for all c. $\square$

Associative Law of Multiplication

Proof. Fix a and b and let S be the set of all c such that the law holds. Note that

$$(xy)\cdot 1=xy=x(y\cdot 1)$$

so that $1\in S$. Let $c\in S$. Then $(ab)c=a(bc)$. Thus

$$(ab)c'=(ab)c+ab=a(bc)+ab=a(bc+b)=a(bc')$$

and $c'\in S$. Thus the law holds for all c. $\square$

Lemma 2. *For $a,b\in\mathbb{N}$ we have $a\neq a+b$.*

Proof. Fix a and let S be the set of all b such that statement is true. We know $1 \neq a' = a + 1$ so $1 \in S$. Let $y \in S$ so that $a \neq a + b$. Then $b' \neq (a + b)' = a + b'$. Thus $b' \in S$ and the statement is true for all b. $\square$

** **Problem 8.** *For $a, b, c \in \mathbb{N}$ show the following:*
1) Exactly one of $a = b$, there exists u such that $a = b + u$, there exists v such that $b = a + v$ is true.
2) If $a < b$ and $b < c$ then $a < c$.
3) If $a < b$ then $a + c < b + c$.

Proof. 1) By Lemma 2, the first and second and first and third conditions cannot both be true. Similarly the second and third conditions cannot both be true since

$$a = b + u = (a + v) + u = a + (v + u).$$

So at most one of the conditions is true for all $a, b \in \mathbb{N}$. Now fix a and let S be the set of all b such that at least one of the conditions holds. For $b = 1$ we have either $a = 1 = b$ or $a = u' = u + 1 = b + u$ for some u. Thus $1 \in S$. Let $b \in S$. Then either $a = b$, so that

$$b' = b + 1 = a + 1$$

and b' satisfies the third condition, or $a = b + u$ so that if $u = 1$ then $a = b + 1 = b'$ and b' satisfies the first condition, else if $u \neq 1$ then for some w, $u = w' = 1 + w$ and

$$a = b + u = b + w' = b + (w + 1) = b + (1 + w) = (b + 1) + w = b' + w$$

and b' satisfies the second condition, or finally $b = a + v$ so that

$$b' = (a + v)' = a + v'$$

and b' satisfies the third condition. In all cases, $b' \in S$ and so the statement holds for all b.

2) Let $a < b$ and $b < c$. Then there exists $v, w \in \mathbb{N}$ such that $b = a + v$ and $c = b + w$. Thus

$$c = (a + v) + w = a + (v + w)$$

and so $a < c$.

3) If $a < b$ then $a + u = b$ for some u. Then

$$b + c = (a + u) + c = (u + a) + c = u + (a + c) = (a + c) + u$$

and so $b + c > a + c$. $\square$

** **Problem 9.** *Let $\sim$ be an equivalence relation on $\mathbb{N} \times \mathbb{N}$ such that $(a, b) \sim (c, d)$ if and only if $a + d = b + c$. Show that the set of equivalence classes of this relation is the set of integers.*

** **Definition 9.1** *Let $\mathbb{Z}$ be the set of equivalence classes of $\sim$. Let $X, Y \in \mathbb{Z}$ such that $(a_1, b_1) \in X$ and $(a_2, b_2) \in Y$. Define*

$$X + Y = \overline{(a_1 + a_2, b_1 + b_2)}$$
$$X \cdot Y = XY = \overline{(a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1)}$$

** **Problem 9.2** *The operations $+$ and $\cdot$ are well defined. That is, if $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$ then*

$$(a_1 + a_2, b_1 + b_2) \sim (c_1 + c_2, d_1 + d_2)$$

and

$$(a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1) \sim (c_1 c_2 + d_1 d_2, c_1 d_2 + c_2 d_1).$$

Proof. Let $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$. Then $a_1 + d_1 = b_1 + c_1$ and $a_2 + d_2 = b_2 + c_2$. Adding these equations gives us

$$(a_1 + a_2) + (d_1 + d_2) = (b_1 + b_2) + (c_1 + c_2)$$

which implies

$$(a_1 + a_2, b_1 + b_2) \sim (c_1 + c_2, d_1 + d_2).$$

A longer calculation can be done to show that

$$a_1 a_2 + b_1 b_2 + c_1 d_2 + c_2 d_1 = a_1 b_2 + a_2 b_1 + c_1 c_2 + d_1 d_2$$

which implies

$$(a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1) \sim (c_1 c_2 + d_1 d_2, c_1 d_2 + c_2 d_1).$$

□

**** Problem 9.3 (Associativity of Addition)** *For all $a, b, c \in \mathbb{Z}$ we have $(a + b) + c = a + (b + c)$.*

Proof. Let $(a_1, a_2) \in a$, $(b_1, b_2) \in b$ and $(c_1, c_2) \in c$. Then we have

$$\begin{aligned}
(a + b) + c &= \left(\overline{(a_1, a_2)} + \overline{(b_1, b_2)}\right) + \overline{(c_1, c_2)} \\
&= \overline{(a_1 + b_1, a_2 + b_2)} + \overline{(c_1, c_2)} \\
&= \overline{((a_1 + b_1) + c_1, (a_1 + b_1) + c_2)} \\
&= \overline{(a_1 + (b_1 + c_1), a_2 + (b_2 + c_2))} \\
&= \overline{(a_1, a_2)} + \overline{(b_1 + c_1, b_2 + c_2)} \\
&= \overline{(a_1, a_2)} + \left(\overline{(b_1, b_2)} + \overline{(c_1, c_2)}\right) \\
&= a + (b + c)
\end{aligned}$$

□

**** Problem 9.4 (Commutativity of Addition)** *For all $a, b \in \mathbb{Z}$ we have $a + b = b + a$.*

Proof. Let $(a_1, a_2) \in a$ and $(b_1, b_2) \in b$. Then

$$a + b = \overline{(a_1, a_2)} + \overline{(b_1, b_2)} = \overline{(a_1 + b_1, a_2 + b_2)} = \overline{(b_1 + a_1, b_2 + a_2)} = \overline{(b_1, b_2)} + \overline{(a_1, a_2)} = b + a.$$

□

**** Problem 9.5 (Additive Identity)** *There exists $n \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$ we have $n + a = a$. From here forward we will call this n, 0.*

Proof. Let $n = \overline{(1, 1)}$. Let $a \in \mathbb{Z}$ such that $(a_1, a_2) \in a$. Then

$$n + a = \overline{(1, 1)} + \overline{(a_1, a_2)} = \overline{(1 + a_1, 1 + a_2)}.$$

Note that $\overline{(1 + a_1, 1 + a_2)} = \overline{(a_1, a_2)}$ because

$$1 + a_1 + a_2 = 1 + a_2 + a_1.$$

□

**** Problem 9.5 (Additive Inverse)** *For all $a \in \mathbb{Z}$ there exists $b \in \mathbb{Z}$ such that $b + a = 0$. From here forward we will call this b, $-a$.*

Proof. Let $a \in \mathbb{Z}$ such that $(a_1, a_2) \in a$ and consider $b = \overline{(a_2, a_1)}$. Then

$$b + a = \overline{(a_2, a_1)} + \overline{(a_1, a_2)} = \overline{(a_2 + a_1, a_1 + a_2)} = \overline{(1, 1)}.$$

□

**** Problem 9.6 (Associativity of Multiplication)** *For all $a, b, c \in \mathbb{Z}$ we have $(ab)c = a(bc)$.*

Proof. Let $(a_1, a_2) \in a$, $(b_1, b_2) \in b$ and $(c_1, c_2) \in c$. Then we have

$$\begin{aligned}
(ab)c &= \left(\overline{(a_1, a_2)} \cdot \overline{(b_1, b_2)}\right) \cdot \overline{(c_1, c_2)} \\
&= \overline{(a_1b_1 + a_2b_2, a_1b_2 + a_2b_1)} \cdot \overline{(c_1, c_2)} \\
&= \overline{((a_1b_1 + a_2b_2)c_1 + (a_1b_2 + a_2b_1)c_2, (a_1b_1 + a_2b_2)c_2 + (a_1b_2 + a_2b_1)c_1)} \\
&= \overline{(a_1b_1c_1 + a_1b_2c_2 + a_2b_2c_1 + a_2b_1c_2, a_2b_2c_2 + a_2b_1c_1 + a_1b_1c_2 + a_1b_2c_1)} \\
&= \overline{(a_1(b_1c_1 + b_2c_2) + a_2(b_1c_2 + b_2c_1), a_2(b_1c_1 + b_2c_2) + a_1(b_1c_2 + b_2c_1))} \\
&= \overline{(a_1, a_2)} \cdot \overline{(b_1c_1 + b_2c_2, b_1c_2 + b_2c_1)} \\
&= \overline{(a_1, a_2)} \cdot \left(\overline{(b_1, b_2)} \cdot \overline{(c_1, c_2)}\right) \\
&= a(bc)
\end{aligned}$$

□

**** Problem 9.7 (Commutativity of Multiplication)** *For all $a, b \in \mathbb{Z}$ we have $ab = ba$.*

Proof. Let $(a_1, a_2) \in a$ and $(b_1, b_2) \in b$. Then

$$ab = \overline{(a_1, a_2)} \cdot \overline{(b_1, b_2)} = \overline{(a_1b_1 + a_2b_2, a_1b_2 + a_2b_1)} = \overline{(b_1a_1 + b_2a_2, b_1a_2 + b_2a_1)} = \overline{(b_1, b_2)} \cdot \overline{(a_1, a_2)} = ba.$$

□

**** Problem 9.8 (Multiplicative Identity)** *There exists $e \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$ we have $ea = a$. From here forward we will call this e, 1.*

Proof. Let $e = \overline{(1 + 1, 1)}$ and let $a \in \mathbb{Z}$ such that $(a_1, a_2) \in a$. Then

$$\begin{aligned}
ea &= \overline{(1 + 1, 1)} \cdot \overline{(a_1, a_2)} \\
&= \overline{((1 + 1)a_1 + 1 \cdot a_2, (1 + 1)a_2 + 1 \cdot a_1)} \\
&= \overline{(a_1 + (a_1 + a_2), a_2 + (a_1 + a_2))} \\
&= \overline{(a_1, a_2)} \\
&= a.
\end{aligned}$$

□

**** Problem 9.9 (Distributivity)** *For all $a, b, c \in \mathbb{Z}$ we have $a(b + c) = ab + ac$.*

Proof. Let $(a_1, a_2) \in a$, $(b_1, b_2) \in b$ and $(c_1, c_2) \in c$. Then we have

$$\begin{aligned}
a(b+c) &= \overline{(a_1, a_2)} \cdot \left(\overline{(b_1, b_2)} + \overline{(c_1, c_2)} \right) \\
&= \overline{(a_1, a_2)} \cdot \overline{(b_1 + c_1, b_2 + c_2)} \\
&= \overline{(a_1(b_1 + c_1) + a_2(b_2 + c_2), a_1(b_2 + c_2) + a_2(b_1 + c_1))} \\
&= \overline{(a_1 b_1 + a_1 c_1 + a_2 b_2 + a_2 c_2, a_1 b_2 + a_1 c_2 + a_2 b_1 + a_2 c_1)} \\
&= \overline{((a_1 b_1 + a_2 b_2) + (a_1 c_1 + a_2 c_2), (a_1 b_2 + a_2 b_1) + (a_1 c_2 + a_2 c_1))} \\
&= \overline{(a_1 b_1 + a_2 b_2, a_1 b_2 + a_2 b_1)} + \overline{(a_1 c_1 + a_2 c_2, a_1 c_2 + a_2 c_1)} \\
&= \overline{(a_1, a_2)} \cdot \overline{(b_1, b_2)} + \overline{(a_1, a_2)} \cdot \overline{(c_1, c_2)} \\
&= ab + ac.
\end{aligned}$$

□

**** Definition 9.10 (Embedding of $\mathbb{N}$)** *Let $f : \mathbb{N} \to \mathbb{Z}$ be a function defined by*

$$f(n) = \overline{(n+1, 1)}.$$

**** Problem 9.11** *The function f is injective.*

Proof. Let $a, b \in \mathbb{N}$ such that $f(a) = f(b)$. Then we have $\overline{(a+1, 1)} = \overline{(b+1, 1)}$ and so $(a+1) + 1 = 1 + (b+1)$ which means that $a = b$. Thus f is injective. □

**** Problem 9.12** *For all $a, b \in \mathbb{N}$ we have*

$$f(a+b) = f(a) + f(b)$$

and

$$f(ab) = f(a)f(b).$$

Proof. Let $a, b \in \mathbb{N}$, then $f(a) = \overline{(a+1, 1)}$ and $f(b) = \overline{(b+1, 1)}$. Then

$f(a+b) = \overline{(a+b+1, 1)} = \overline{((a+b+1)+1, 1+1)} = \overline{((a+1)+(b+1), 1+1)} = \overline{(a+1, 1)} + \overline{(b+1, 1)} = f(a) + f(b)$.

Similarly,

$$\begin{aligned}
f(ab) &= \overline{(ab+1, 1)} \\
&= \overline{(ab+1+a+b+1, a+b+1+1)} \\
&= \overline{((a+1)(b+1)+1, (a+1)+(b+1))} \\
&= \overline{(a+1, 1)} \cdot \overline{(b+1, 1)} \\
&= f(a)f(b).
\end{aligned}$$

□

**** Definition 9.13** *Let $a, b \in \mathbb{Z}$ such that $(a_1, a_2) \in a$ and $(b_1, b_2) \in b$. Then*

$$a < b \text{ if } a_1 + b_2 < a_2 + b_1.$$

**** Problem 9.14** *The relation $<$ is well-defined.*

Proof. Let $\overline{(a_1, a_2)}, \overline{(b_1, b_2)}, \overline{(c_1, c_2)}, \overline{(d_1, d_2)} \in \mathbb{Z}$ such that $\overline{(a_1, a_2)} < \overline{(b_1, b_2)}$, $\overline{(a_1, a_2)} \sim \overline{(c_1, c_2)}$ and $\overline{(b_1, b_2)} \sim \overline{(d_1, d_2)}$. Then we know that

$$a_1 + b_2 < a_2 + b_1,$$

$$a_1 + c_2 = a_2 + c_1$$

and

$$b_1 + d_2 = b_2 + d_1.$$

Adding the desired quantities to the inequality results in

$$a_1 + a_2 + b_1 + b_2 + c_1 + d_2 < a_1 + a_2 + b_1 + b_2 + c_2 + d_1$$

which gives us the result

$$\overline{(c_1, c_2)} < \overline{(d_1, d_2)}.$$

□

**** Problem 9.15** *The relation $<$ is an ordering on $\mathbb{Z}$.*

Proof. Let $(a_1, a_2) \in a$, $(b_1, b_2) \in b$ and $(c_1, c_2) \in c$. Then it's clear that if $a < b$ then

$$a_1 + b_2 < a_2 + b_1$$

and so $a \neq b$ and a is not greater than b. The same argument holds for $a > b$. Note that a must be at least greater than, less than or equal to b however, because of the ordering of $\mathbb{N}$.

Suppose that $a < b$ and $b < c$. Then we have

$$a_1 + b_2 < a_2 + b_1$$

and

$$b_1 + c_2 < b_2 + c_1.$$

Adding these gives the desired result that

$$a_1 + c_2 < a_2 + c_1$$

so $a < c$.

Suppose that $a < b$. Then $a + c = \overline{(a_1 + c_1, a_2 + c_2)}$ and $b + c = \overline{(b_1 + c_1, b_2 + c_2)}$. Since

$$a_1 + b_2 < a_2 + b_1$$

it's clear that

$$a_1 + b_2 + c_1 + c_2 < a_2 + b_1 + c_1 + c_2$$

which shows that $a + c < b + c$.

Finally, suppose that $a < b$ and $0 < c$. Then $a_1 + b_2 < a_2 + b_1$ and $c_2 < c_1$. Combining these inequalities gives us the desired result of

$$(a_1c_1 + a_2c_2) + (b_1c_2 + b_2c_1) < (a_1c_2 + a_2c_1) + (b_1c_1 + b_2c_2)$$

which implies that $ac < bc$. □

**** Problem 9.16** *For all $n \in \mathbb{N}$, we have $f(n) > 0$. Additionally, if $a \in \mathbb{Z}$ such that $a > 0$, then $a = f(n)$ for some $n \in \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$. Then $f(n) = \overline{(n+1, 1)}$ and $n + 2 > 2$. Thus $f(n) > 0$.

Let $a \in \mathbb{Z}$ such that $(a_1, a_2) \in a$ and $a > 0$. Then $a_1 > a_2$ so there exists some b such that $\overline{(a_1, a_2)} = \overline{(a_1 + b, 1)}$ so that $a = f(n)$ for some $n \in \mathbb{N}$. ∎

Thus there is a bijection between $\mathbb{N}$ and the positive elements of $\mathbb{Z}$. Hence, $\mathbb{Z}$ is a ordered integral domain where the positive elements are well ordered.