Homework 2 Solutions

September 10, 2023

Section 1.2

Problem 1.2.3

(a) This is false; let $A_n = \{n, n+1, n+2, \dots\}$ for $n \in \mathbb{N}$ so that $A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots$. Then $\bigcap_{n=1}^{\infty} A_n = \emptyset$ and in particular is not infinite.

(b) This is true (finiteness is important).

(c) This is false. Consider $A = B = \{1\}$ and $C = \{2\}$. Then $A \cap (B \cup C) = \{1\}$ but $(A \cap B) \cup C = \{1, 2\}$.

(d) This is true.

(e) This is true.

1.2.5(c)

We want to show that if $A, B \subset C$, then $(A \cup B)^c = A^c \cap B^c$.

First let $x \in (A \cup B)^c$. Then $x \notin A \cup B$, which means that $x \notin A$ and $x \notin B$. Hence $x \in A^c$ and $x \in B^c$, so $x \in A^c \cap B^c$. As x was arbitrary, we have that $(A \cup B)^c \subseteq A^c \cap B^c$.

In the other direction, let $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$, implying that $x \notin A$ and $x \notin B$. Hence $x \notin A \cup B$, and therefore $x \in (A \cup B)^c$. As x was arbitary, we have that $A^c \cap B^c \subseteq (A \cup B)^c$.

As we have shown inclusions in both directions, we conclude that the two sets are equal.

Other Problems

Problem 5

(a) Suppose that $b \in f(C \cap D)$. Then by definition of the image of a set, there must be some $x \in C \cap D$ such that $f(x) = b$. Now, $x \in C$, so it must be the case that $b = f(x) \in f(C)$. But also $x \in D$, so $b = f(x) \in f(D)$. We see that in fact $b \in f(C) \cap f(D)$. As b was an arbitary element of $f(C \cap D)$, we conclude that $f(C \cap D) \subseteq f(C) \cap f(D)$.

(b) Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. Suppose that $C = [0, 1]$, and $D = [-1, 0]$, such that $f(C \cap D) = f(\{0\}) = \{0\}$. But $f(C) = f(D) = [0, 1]$, so we see that $f(C) \cap f(D) = [0, 1]$. Hence $f(C \cap D)$ is a proper subset of $f(C) \cap f(D)$.

Problem 6

(a) Given (m, n) such that $m, n \in \mathbb{Z}$ and $n \neq 0$, our proposed equivalence relation $\sim$ is that $(m, n) \sim (m', n')$ if $mn' = m'n$. We check three properties:

(i) Reflexivity. We observe that $mn = mn$, so $(m, n) \sim (m, n)$.

(ii) Symmetry. If we have $(m, n) \sim (m', n')$, then $mn' = m'n$. But multiplication commutes in the integers, so in fact $n'm = nm'$. Hence $(m', n') \sim (m, n)$.

(iii) Transitivity. If we have $(m, n) \sim (m', n')$ and $(m', n') \sim (m'', n'')$, then $mn' = m'n$ and $m'n'' = m''n'$. There are two cases. First, if $m' = 0$, then since $n, n', n'' \neq 0$, for the preceding equations to be true, we must also have $m = m'' = 0$. Then certainly $mn'' = m''n$, so we have that $(m, n) \sim (m'', n'')$. In the other case, if $m' \neq 0$, then multiplying the two previous equations we conclude that $mn'm'n'' = m'nm''n'$. As $n', m' \neq 0$, we may divide through to obtain $mn'' = nm''$, and conclude that $(m, n) \sim (m'', n'')$.

(b) Recall that addition is given by

$$[(m, n)] + [(p, q)] = [(mq + np, nq)].$$

Since this operation clearly commutes, it suffices to check that if $(m, n) \sim (m', n')$, or in other words if $mn' = nm'$, it follows that $(mq + np, nq) \sim (m'q + n'p, n'q)$ for any (p, q) with $q \neq 0$. In particular we would like to show that

$$(mq + np)n'q = nq(m'q + n'p)$$

which expands to $mn'pq + nn'pq = m'npq + nn'pq$. This is indeed true if $mn' = m'n$, so we are satisfied.

Next we consider multiplication. It again suffices to check that if $(m, n) \sim (m', n')$, or in other words if $mn' = nm'$, it follows that $(mp, nq) \sim (m'p, n'q)$. This requires that $mpn'q = nqm'p$, which is indeed true if $mn' = nm'$. So we are satisfied that multiplication is well-defined.

Problem 7

(a) We must first satisfy ourselves that these operations are well-defined. Suppose that $[a] = [a']$, so that $a - a' = nk$, and $b - b' = mk$, where n and m are some integers. Then we observe that $(a + b) - (a' + b') = (a - a') + (b - b') = nk + mk = (n + m)k$. Since $n + m$ is an integer, we conclude that $[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$. Hence, addition is well-defined.

Now we turn our attention to multiplication. We observe that $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') = nkb + a'mk = k(nb + a'm)$. As n, m, b, a' are integers, we see that $nb + a'm$ is an integer, so in fact $[a][b] = [ab] = [a'b'] = [a'][b']$.

Having checked well-definedness, the field axioms are mostly straightforward consequences of corresponding properties in $\mathbb{Z}$, with the exception of existence of multiplicative inverses. We proceed through them.

(A1) For all $[a], [b], [c]$ in $\mathbb{Z}/k\mathbb{Z}$, we have that $[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c]$.

(A2) For all $[a], [b] \in \mathbb{Z}/k\mathbb{Z}$, we have $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.
(A3) The additive identity element is $[0]$, since for all $[a] \in \mathbb{Z}/k\mathbb{Z}$, we have $[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a]$.
(A4) The additive inverse $-[a]$ of $[a] \in \mathbb{Z}/k\mathbb{Z}$ is the element $[-a] = [p - a]$, since $[a] + [-a] = [a + (-a)] = [0] + [(-a) + a] = [-a] + [a]$.
(M1) For all $[a], [b], [c]$ in $\mathbb{Z}/k\mathbb{Z}$, we have $[a]([b][c]) = [a]([bc]) = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c]$.
(M2) For all $[a], [b] \in \mathbb{Z}/k\mathbb{Z}$, we have $[a][b] = [ab] = [ba] = [b][a]$.
(M3) The multiplicative identity element is $[1]$, since for all $[a] \in \mathbb{Z}/k\mathbb{Z}$, we have $[a][1] = [a(1)] = [a] = [1(a)] = [1][a]$.
(DL) For all $[a], [b], [c] \in \mathbb{Z}\ k\mathbb{Z}$, we have $[a]([b] + [c]) = [a]([b + c]) = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$.

(b) Observe that in $\mathbb{Z}/4\mathbb{Z}$, there is no multiplicative inverse of $[2]$. For, indeed, $[2][0] = [0]$, $[2][1] = [2]$, $[2][2] = [4] = [0]$, and $[2][3] = [6] = [2]$, and none of these is $[1]$. More abstractly, we note that for any integer a, $2a$ is even; but if $[b] = [1]$, then $b - 1 = 4n$ for some integer n, so we have $b = 4n + 1$, which is odd.

(c) Let $[a] \neq [0]$ in $\mathbb{Z}/p\mathbb{Z}$. Note that $[a]$ is not divisible by $[p]$. Recall that the elements of $\mathbb{Z}/p\mathbb{Z}$ can be listed as $\{[0], \ldots, [p-1]\}$. Consider the elements $\{[a(0)], \ldots, [a(p-1)]\}$. We claim these p elements are distinct. For, suppose that $[ab] = [ac]$ for some $0 \leq b < c \leq p - 1$. Then $ab - ac = a(b - c)$ is divisible by p. But a is not divisible by p, and $b - c$ is a nonzero integer with $-(p-1) \leq b - c \leq p - 1$, and therefore also not divisible by p. So, this is a list of p distinct elements of $\mathbb{Z}/p\mathbb{Z}$. One of the elements on this list $[a][b]$ must then be $[1]$. By commutativity, it is also true that $[b][a] = [1]$. So, $[b]$ is the multiplicative inverse of $[a]$.

(d) In $\mathbb{Z}/3\mathbb{Z}$, we have $[2][2] = [4] = [1]$, so the multiplicative inverse of $[2]$ is $[2]$. In $\mathbb{Z}/5\mathbb{Z}$, we have $[2][3] = [6] = [1]$, so the multiplicative inverse of $[2]$ is $[3]$.