Math 115AH Homework 1

April 10, 2024

1. **Problem 1**

   (a) **Prove the sum of two odd numbers is an even number.**
   Let $m, n \in \mathbb{Z}$ such that $m = 2j + 1$ and $n = 2k + 1$ for some $j, k \in \mathbb{Z}$. Then by definition. m, n are odd integers. Then

   $$m + n = (2j + 1) + (2k + 1) = 2(j + k + 1)$$

   Therefore $\exists$ some $a \in \mathbb{Z}$ such that $m + n = 2a$ for all m, n, which by definition makes $m + n$ an even integer.

   (b) **Prove the sum of an odd number and even number is an odd number**
   Let $m, n \in \mathbb{Z}$ such that m is even and n is odd. Then $m = 2j$ and $n = 2k + 1$ for some $j, k \in \mathbb{Z}$
   Then

   $$m + n = 2j + 2k + 1 = 2(j + k) + 1$$

   Therefore $\exists$ some $a \in \mathbb{Z}$ such that $m + n = 2a + 1$ for all m, n. This means $m + n$ must be an odd integer.

2. **Problem 2**

   (a) **What is the union of the set of all even integers and the set of all odd integers?**
   The set of all integers

   (b) **What is the intersection of the set of all even integers and the set of all odd integers?**
   $\emptyset$

   (c) **Is the empty set a subset of the set of all even integers?**
   Yes it is. The empty set is a subset of all sets

3. **Problem 3**

   (a) **Let A and B be arbitrary sets. Prove that $A \cap B \subset A$.**
   Let x $\in$ A $\cap$ B, then A $\cap$ B = {x | x $\in$ A and x $\in$ B}.
   Then by definition of intersection, x $\in$ A.

4. **Problem 4**

   (a) **Explain why the definition for one-to-one is equivalent to saying that f takes distinct elements in S to distinct values in T.**
   A one-to-one function requires that if $f(x_1) = f(x_2)$, then $x_1 = x_2$. This means that every element in S maps to a distinct element in T.

   (b) **Give examples in what follows:**

   i. **Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ that is one-to-one but not onto.**
   The function $f : \mathbb{N} \to \mathbb{N}$ where $f(x) = x^2$ is injective but not surjective

   ii. **Give an example of a function $g : \mathbb{R} \to \mathbb{R}$ that is onto but not one-to-one**
   The function $g : \mathbb{Z} \to \mathbb{N}$ where $g = |x| + 1$ is surjective but not injective

   iii. **Give the formula for $f \circ g : \mathbb{R} \to \mathbb{R}$ for the examples that you defined above**
   $f \circ g = (|x| + 1)^2$

   (c) **Given functions $f : S \to T$ and $g : R \to S$, prove the following statements:**

   i. **If f and g are both onto, then $f \circ g$ is onto.**
   Since $f \circ g = f(g)$, we have $f \circ g : R \to S \to T$
   If f is onto, then $\forall t \in T$, $\exists$ some $s \in S$ such that $f(s) = t$. Similarly, If g is onto, then $\forall s \in S$, $\exists$ some $r \in R$ such that $g(r) = s$. This means that as g is onto, every element in S has a preimage in R. Furthermore, since every element of S has an image in T and every element of T has a preimage in S, there must be a preimage in R for all elements in T, which shows that $f \circ g$ must be onto

ii. **If f and g are both one-to-one, then $f \circ g$ is one-to one.**
If f is injective, then every element in S has a distinct image in T. Similarly, if g is injective, then every element in R has a distinct image in S. Therefore, $f \circ g$ sends each element of R to a distinct image in T.

iii. **If f and g are both bijections, then $f \circ g$ is a bijection**
If f is bijective, then each element in T has a single unique preimage in S. It then follows that if g is bijective, each element in S has a single unique preimage in R. Since every element in S has also has a distinct image in T from f, every element in T must have a single distinct preimage in R.

5. **Problem 5**

(a) **Prove that, in any field F, additive inverses are unique. That is, if $a \in F$ and b, b' both satisfy that $a + b = 0_F$ and $a + b' = 0_F$, then $b = b'$**
Suppose $a+b = 0_F$, then $a+b+b' = 0_F + b' = a+b'+b$. Since we know $a+b' = 0_F$, we have that $0_F + b' = 0_F + b$. Therefore, $b' = b$.

6. **Problem 6**

(a) **Let S be a set with an equivalence relation $R \subset S \times S$. Let $f : S \to T$ be a function. Suppose also that if $x, y \in S$ and $x \sim_R y$, then $f(x) = f(y)$. Recall from discussion that S/R is defined to be the set of all equivalence classes of elements in S. Prove that there exists a unique function $\bar{f} : S/R \to T$ such that $\bar{f}([x]) = f(x)$.**
Notice that if $x \sim_R y$, then $y \in [x]$. Then $\forall a, b \in [x], f(a) = f(b) \implies f$ maps every element of an equivalence class to the same element in T. We know that $\bar{f}$ maps an entire equivalence class in S to one element in T. Therefore $\bar{f}([x]) = f(x)$ exists and is well-defined as $\bar{f}$ and f have the same codomain.
Now suppose there exist functions $\bar{f} : S/R \to T$ and $\bar{g} : S/R \to T$ such that $\bar{f}([x]) = f(x)$ and $\bar{g}([x]) = f(x)$. S/R is defined as the set of all equivalence classes of elements in S. Therefore, every element in S/R exists in the form $[x] \in S/R$. Since we established earlier that $f(a) = f(b)\ \forall a, b \in [x]$, observe that $\forall [x] \in S/R, \bar{f}([x]) = f(a)$ and $\bar{g}([x]) = f(a)\ \forall a \in [x]$. Therefore $\bar{f}(c) = \bar{g}(c)\ \forall c \in S/R \implies \bar{f} = \bar{g}. \implies \bar{f}$ is unique.

7. **Problem 7**

(a) **What is the additive identity of $\mathbb{C}$? What is the multiplicative identity of $\mathbb{C}$?**
The additive identity is the real number 0, represented as $0 + 0i$. The multiplicative identity is the real number 1, represented as $1 + 0i$

(b) **Find the additive inverse of the element $2 + i \in \mathbb{C}$.**
$(-2) + (-i)$

(c) **Find the multiplicative inverse of the element $1 + 4i \in \mathbb{C}$**
$\frac{1}{17} - \frac{4}{17}i$

(d) **Give a general formula for the multiplicative inverse of a complex number $a + bi$, for $a, b \in \mathbb{R}$ with at least one of a or b nonzero.**

$$(a + bi)^{-1} = \left(\frac{a}{a^2 + b^2}\right) - \left(\frac{b}{a^2 + b^2}\right) i$$

(e) **Prove that the set $\mathbb{C}$ with operation $+$ and $\cdot$ defined by (1) and (2) above satisfies the axioms (F1) and (F5).**
Let $a + bi, c + di \in \mathbb{C}$. Then $(a + bi) +_F (c + di) = (a + c) +_F (b + d)i$ and $(c + di) +_F (a + bi) = (c + a) +_F (d + b)i$. For $a, b \in \mathbb{R}, a + b = b + a$. Therefore, $a + c = c + a$ and $b + d = d + b \implies (a + bi) +_F (c + di) = (c + di) +_F (a + bi)$ Additionally, $(a + bi) \cdot_F (c + di) = (ac - bd) +_F i(ad + bc)$ and $(c + di) \cdot_F (a + bi) = (ca - db) +_F i(da + cb)$ Similarly, for $a, b \in \mathbb{R}, a \cdot b = b \cdot a$. Hence, $ac = ca$ and $bd = db \implies (a + bi) \cdot_F (c + di) = (c + di) \cdot_F (a + bi) \implies$ the set $\mathbb{C}$ satisfies (F1).
Let $a + bi, c + di, e + fi \in \mathbb{C}$. Then $(a + bi) \cdot_F ((c + di) +_F (e + fi)) = (a + bi) \cdot_F ((c + e) +_F (d + f)i) = (a(c + e) - b(d + f)) +_F i(a(d + f) + b(c + e)) = (ac + ae - bd - bf) +_F i(ad + af + bc + be)$
By (F5), $a + bi \cdot_F ((c + di) +_F (e + fi)) = ((a + bi) \cdot_F (c + di)) +_F ((a + bi) \cdot_F (e + fi)) = ((ac - bd) + i(ad + bc)) +_F ((ae - bf) + i(af + be)) = (ac + ae - bd - bf) +_F i(ad + af + bc + be)$. Therefore the set $\mathbb{C}$ satisfies (F5).

8. **Problem 8**

(a) **Suppose that $[x] = [y]$ and $[z] = [w]$ for some $x, y, z, w \in \mathbb{Z}$**

i. **Show that $[x + z] = [y + w]$**
$[x + z] = [x] +_n [z] = [y] +_n [w] = [y + w]$

ii. **Show that $[x \cdot z] = [y \cdot w]$**
$[x \cdot z] = [x] \cdot_n [z] = [y] \cdot_n [w] = [y \cdot w]$

(b) **Let p be a prime number, meaning that p has no positive divisors except 1 and p itself. Prove that $\mathbb{Z}/p\mathbb{Z}$, with operations defined on WS1, is a field**
Recall that $\mathbb{Z}/p\mathbb{Z} = \{[0], [1], [2], ..., [p-1]\}$.

i. For all $[a], [b] \in \mathbb{Z}/p\mathbb{Z}$, $[a] +_p [b] = [a+b] = [b+a] = [b] +_p [a]$ and $[a] \cdot_p [b] = [a \cdot b] = [b \cdot a] = [b] \cdot_p [a]$

ii. For all $[a], [b], [c] \in \mathbb{Z}/p\mathbb{Z}$, $([a] +_p [b]) +_p [c] = [a+b] +_p [c] = [a+b+c] = [a] +_p [b+c] = [a] +_p ([b] +_p [c])$

iii. $[0] +_p [a] = [0+a] = [a]$ and $[1] \cdot_p [a] = [1 \cdot a] = [a]$ $\forall [a] \in \mathbb{Z}/p\mathbb{Z}$

iv. For all $[a] \in \mathbb{Z}/p\mathbb{Z}, \exists\ [b] \in \mathbb{Z}/p\mathbb{Z}$ such that $[a] +_p [b] = [a+b] = [p] = [0]$
To show the multiplicative inverse exists, use the fact that $\exists x, y \in \mathbb{Z}$ such that $xa + yb = \gcd(a, b)$.
Suppose you have an arbitrary nonzero element $a \in \mathbb{Z}/p\mathbb{Z}$, then $\gcd(a, p) = 1$ since p is prime. Then $\exists x, y \in \mathbb{Z}$ such that $xa +_p yp = 1 \implies [x \cdot a] +_p [y \cdot p] = [x \cdot a] = [a \cdot x] = [a] \cdot [x] = [1]$ since $[y \cdot p] = [p] = [0]$. Therefore for all nonzero elements in $\mathbb{Z}/p\mathbb{Z}, \exists$ an $x \in \mathbb{Z}$ such that $[a] \cdot [x] = [1]$

v. For all $[a], [b], [c] \in \mathbb{Z}/p\mathbb{Z}$, $[a] \cdot_p ([b] +_p [c]) = [a] \cdot_p [b+c] = [a \cdot (b+c)] = [a \cdot b + a \cdot c] = [a \cdot b] +_p [a \cdot c] = [a] \cdot_p [b] +_p [a] \cdot_p [c]$

(c) **A number n is called a *composite number* if there exists positive integers $k, m > 1$ such that $n = km$. Prove that $[1]$ is a multiplicative identity for $\mathbb{Z}/p\mathbb{Z}$, even when n is composite. Prove that the element $[k] \in \mathbb{Z}/p\mathbb{Z}$ does not have a multiplicative inverse.**

i. Let n be a composite number such that $n = km$ as defined. Suppose you choose an arbitrary element $[x] \in \mathbb{Z}/p\mathbb{Z}$ such that x is not a factor of n, then $[x] \cdot [1] = [x \cdot 1] = [x]$. Now suppose you choose an arbitrary element $[k] \in \mathbb{Z}/p\mathbb{Z}$ such that k is a factor of n and $n = km$. The identity still holds, as $[k] \cdot [1] = [k]$.

ii. Assume $[k]$ has a multiplicative inverse, then $\exists\ [l] \in \mathbb{Z}/p\mathbb{Z}$ such that $[k] \cdot_n [l] = 1$. Let $[k] = [nj_1 + k]$ for some $j_1 \in \mathbb{Z}$, and that $m \cdot k = n$ for some integer $m > 1$. Then, suppose $\exists\ c \in \mathbb{Z}$ such that $[c] = [nj_2 + c] \in \mathbb{Z}/p\mathbb{Z}$ for some $j_2 \in \mathbb{Z}$ and $[c]$ is the multiplicative inverse of $[k]$. Then, we have that

$$
\begin{aligned}
[k] \cdot_n [c] &= [(nj_1 + k) \cdot (nj_2 + c)] \\
&= [n(.......) + k \cdot c] = [k \cdot c] \\
&= [1]
\end{aligned}
$$

However, considering that k is a factor of n, notice that $[k \cdot c] \in \{[kd] : d \in \mathbb{Z}, 0 \leq d < \frac{n}{k}\}$. This means that $\exists$ the multiplicative inverse c such that $[k \cdot c] = [k] \cdot [c] = [1]$ only when $[1] \in \{[kd] : d \in \mathbb{Z}, 0 \leq d < \frac{n}{k}\}$, or when $k = 1$. However, we defined k to be greater than 1, hence $[k]$ cannot have a multiplicative inverse by contradiction.