Math 3450 - Homework # 3
Well-Defined Operations

1. Show that the operation $\overline{a} \oplus \overline{b} = \overline{a}^2 + \overline{b}^2$ is a well-defined operation for $\mathbb{Z}_n$. Here $\overline{a}^2$ means $\overline{a} \cdot \overline{a}$. For example, in $\mathbb{Z}_4$ we have that

$$\overline{2} \oplus \overline{3} = \overline{2} \cdot \overline{2} + \overline{3} \cdot \overline{3} = \overline{4} + \overline{9} = \overline{1}.$$

Proof. 1) Let $\overline{a}, \overline{b} \in \mathbb{Z}_n$ where $a, b \in \mathbb{Z}$.

Then
$$\overline{a} \oplus \overline{b} = \overline{a}^2 + \overline{b}^2 = \overline{a^2} + \overline{b^2} = \overline{a^2 + b^2}.$$

Since $a, b \in \mathbb{Z}$ we have that $a^2 + b^2 \in \mathbb{Z}$.

Therefore, $\overline{a} \oplus \overline{b} = \overline{a^2 + b^2} \in \mathbb{Z}_n$.

So $\mathbb{Z}_n$ is closed under the operation $\oplus$.

2) Suppose that $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$. We need to show that $\overline{a_1} \oplus \overline{b_1} = \overline{a_2} \oplus \overline{b_2}$.

From class we had a theorem that says that if $\overline{x} = \overline{y}$ and $\overline{w} = \overline{z}$, then $\overline{x} + \overline{w} = \overline{y} + \overline{z}$ and $\overline{x} \cdot \overline{w} = \overline{y} \cdot \overline{z}$.

Repeatedly using the above theorem we get the following.

We have that $\overline{a_1} \cdot \overline{a_1} = \overline{a_2} \cdot \overline{a_2}$ by multiplying the equations $\overline{a_1} = \overline{a_2}$ and $\overline{a_1} = \overline{a_2}$.

Similarly, $\overline{b_1} \cdot \overline{b_1} = \overline{b_2} \cdot \overline{b_2}$ by multiplying the equations $\overline{b_1} = \overline{b_2}$ and $\overline{b_1} = \overline{b_2}$.

Adding the two equations above we get that $\overline{a_1} \cdot \overline{a_1} + \overline{b_1} \cdot \overline{b_1} = \overline{a_2} \cdot \overline{a_2} + \overline{b_2} \cdot \overline{b_2}$.

Therefore, $\overline{a_1} \oplus \overline{b_1} = \overline{a_2} \oplus \overline{b_2}$.

Thus $\oplus$ is a well-defined operation on $\mathbb{Z}_n$. $\square$

2. Given two integers a and b, let $\min(a, b)$ denote the minimum (smaller) of a and b. Let n be an integer with $n \geq 2$. Is the operation $\overline{a} \oplus \overline{b} = \overline{\min(a, b)}$ a well-defined operation on $\mathbb{Z}_n$?

Solution: This operation is not well-defined. For example, consider $n = 4$. In $\mathbb{Z}_4$ we have that $\overline{0} = \overline{8}$ and $\overline{1} = \overline{5}$. Thus, for the operation to be well-defined we would need $\overline{0} \oplus \overline{1} = \overline{8} \oplus \overline{5}$. However, $\overline{0} \oplus \overline{1} = \overline{\min(0, 1)} = \overline{0}$ and $\overline{8} \oplus \overline{5} = \overline{\min(8, 5)} = \overline{5}$. But $\overline{0} \neq \overline{5}$ in $\mathbb{Z}_4$.

3. (a) Show that the operation $\frac{a}{b} \oplus \frac{c}{d} = \frac{ad}{bc}$ is not a well-defined operation on $\mathbb{Q}$.

   Solution: We have that $\frac{5}{2}, \frac{0}{1} \in \mathbb{Q}$ however $\frac{5}{2} \oplus \frac{0}{1} = \frac{5 \cdot 1}{2 \cdot 0} = \frac{5}{0} \notin \mathbb{Q}$. Hence $\mathbb{Q}$ is not closed under $\oplus$ and the operation is not well-defined.

   (b) Is the operation well-defined on $\mathbb{Q} - \{0\}$?

4. Is the operation $\overline{a} \oplus \overline{b} = \overline{a^b}$ a well-defined operation on $\mathbb{Z}_n$?

   Solution: There are two issues with this operation.

   One issue is as follows. As an example, consider $n = 4$. In $\mathbb{Z}_4$ we have that $\overline{1} = \overline{5}$. Thus, for the operation to be well-defined we must have that $\overline{2} \oplus \overline{1} = \overline{2} \oplus \overline{5}$. However, $\overline{2} \oplus \overline{1} = \overline{2^1} = \overline{2}$ and $\overline{2} \oplus \overline{5} = \overline{2^5} = \overline{32} = \overline{0}$. And $\overline{2} \neq \overline{0}$ in $\mathbb{Z}_4$.

   Another issue is when b is a negative integer. For example, in $\mathbb{Z}_4$ suppose we want to calculate $\overline{2} \oplus \overline{-1}$. What does this mean? The formula says that it is $\overline{2^{-1}}$. But what is that in $\mathbb{Z}_4$? In fact there is no way to make sense of $1/2$ in $\mathbb{Z}_4$ because there is no multiplicative inverse for $\overline{2}$ in $\mathbb{Z}_4$. (Why?) Because there is no $\overline{x} \in \mathbb{Z}_4$ with $\overline{x} \cdot \overline{2} = \overline{1}$. We can check:

   $\overline{0} \cdot \overline{2} = \overline{0} \neq \overline{1}$

   $\overline{1} \cdot \overline{2} = \overline{2} \neq \overline{1}$

   $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0} \neq \overline{1}$

   $\overline{3} \cdot \overline{2} = \overline{6} = \overline{2} \neq \overline{1}$

   Thus there is no way to define $\overline{2^{-1}}$ in $\mathbb{Z}_4$.

5. (Constructing the rational numbers from the integers) Let $S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Define the relation $\sim$ on S where $(a, b) \sim (c, d)$ if and only if $ad = bc$. In the last homework you showed that this is an equivalence relation on S.

   (a) Define the operation $\overline{(a, b)} \oplus \overline{(c, d)} = \overline{(ad + bc, bd)}$. Prove that $\oplus$ is well-defined on the set of equivalence classes.

   Proof. 1) Consider two equivalence classes $\overline{(a, b)}$ and $\overline{(c, d)}$ where $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$.

Then $ad+bc \in \mathbb{Z}$ because $a, b, c, d \in \mathbb{Z}$ and the integers are closed under addition and multiplication.
Also, since $b, d \in \mathbb{Z}-\{0\}$ we have that $bd \neq 0$ and so $bd \in \mathbb{Z}-\{0\}$.
Thus $(ad+bc, bd) \in \mathbb{Z}\times(\mathbb{Z}-\{0\})$ and $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(ad+bc, bd)}$ is a valid equivalence class.

2) Now suppose that $\overline{(a,b)}$,$\overline{(c,d)}$,$\overline{(x,y)}$,and $\overline{(w,z)}$ are equivalence classes in $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$.
Further suppose that $\overline{(a,b)} = \overline{(x,y)}$ and $\overline{(c,d)} = \overline{(w,z)}$.
We need to show that $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(x,y)} \oplus \overline{(w,z)}$.
That is, we need to show that $\overline{(ad+bc, bd)} = \overline{(xz+yw, yz)}$.
The above is equivalent to showing that $(ad+bc)yz = bd(xz+yw)$.
Let's do this.
Since $\overline{(a,b)} = \overline{(x,y)}$ we have that $ay = bx$.
Since $\overline{(c,d)} = \overline{(w,z)}$ we have that $cz = dw$.
Therefore, using the equations $ay = bx$ and $cz = dw$ we get that

$$\begin{aligned} (ad+bc)yz &= adyz + bcyz \\ &= (ay)(dz) + (cz)(by) \\ &= (bx)(dz) + (dw)(by) \\ &= bd(xz+yw). \end{aligned}$$

Thus, $\overline{(ad+bc, bd)} = \overline{(xz+yw, yz)}$.
Thus, the operation $\oplus$ is well-defined on the equivalence classes of $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$.

□

(b) Define the operation $\overline{(a,b)} \odot \overline{(c,d)} = \overline{(ac, bd)}$. Prove that $\odot$ is well-defined on the set of equivalence classes.

Proof. 1) Consider two equivalence classes $\overline{(a,b)}$ and $\overline{(c,d)}$ where $(a,b),(c,d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$.
Then $ac \in \mathbb{Z}$ because $a, c \in \mathbb{Z}$ and the integers are closed under multiplication.
Also, since $b, d \in \mathbb{Z}-\{0\}$ we have that $bd \neq 0$ and so $bd \in \mathbb{Z}-\{0\}$.

Thus $(ac, bd) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ and $\overline{(a,b)} \odot \overline{(c,d)} = \overline{(ac,bd)}$ is a valid equivalence class.

2) Now suppose that $\overline{(a,b)}$,$\overline{(c,d)}$,$\overline{(x,y)}$,and $\overline{(w,z)}$ are equivalence classes in $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$.
Further suppose that $\overline{(a,b)} = \overline{(x,y)}$ and $\overline{(c,d)} = \overline{(w,z)}$.
We need to show that $\overline{(a,b)} \odot \overline{(c,d)} = \overline{(x,y)} \odot \overline{(w,z)}$.
That is, we need to show that $\overline{(ac,bd)} = \overline{(xw,yz)}$.
The above is equivalent to showing that $(ac)(yz) = (bd)(xw)$.
Let's do this.
Since $\overline{(a,b)} = \overline{(x,y)}$ we have that $ay = bx$.
Since $\overline{(c,d)} = \overline{(w,z)}$ we have that $cz = dw$.
Therefore, using the equations $ay = bx$ and $cz = dw$ we get that

$$(ac)(yz) = (ay)(cz) = (bx)(dw) = (bd)(xw).$$

Thus, $\overline{(ac,bd)} = \overline{(xw,yz)}$.
Therefore, the operation $\odot$ is well-defined on the equivalence classes of $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$.

□

6. (Constructing the integers from the natural numbers) Let $S = \mathbb{N} \times \mathbb{N}$. Define the relation $\sim$ on S where $(a,b) \sim (c,d)$ if and only if $a+d = b+c$. In the last homework you showed that this is an equivalence relation on S.

   (a) Define the operation $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$. Prove that $\oplus$ is well-defined on the set of equivalence classes.

   Proof. 1) Consider two equivalence classes $\overline{(a,b)}$ and $\overline{(c,d)}$ where $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$.
   Then $a + c$ and $b + d$ are both in $\mathbb{N}$ because $\mathbb{N}$ is closed under addition.
   Thus, $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$ is a valid equivalence class in $\mathbb{N} \times \mathbb{N}/\sim$.

   2) Now suppose that $\overline{(a,b)}$,$\overline{(c,d)}$,$\overline{(e,f)}$,and $\overline{(g,h)}$ are equivalence classes of $\mathbb{N} \times \mathbb{N}/\sim$.

Further suppose that $\overline{(a,b)} = \overline{(e,f)}$ and $\overline{(c,d)} = \overline{(g,h)}$.
We need to show that $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(e,f)} \oplus \overline{(g,h)}$.
We have that $a + f = b + e$ since $\overline{(a,b)} = \overline{(e,f)}$.
We also have that $c + h = d + g$ since $\overline{(c,d)} = \overline{(g,h)}$.
Adding these two equations gives $a + f + c + h = b + e + d + g$.
Rearranging gives $(a + c) + (f + h) = (b + d) + (e + g)$.
Therefore, $\overline{(a + c, b + d)} = \overline{(e + g, f + h)}$.
Hence $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(e,f)} \oplus \overline{(g,h)}$.

The above arguments show that $\oplus$ is a well-defined operation on the equivalence classes of $\mathbb{N} \times \mathbb{N}/\sim$.

$\square$