Topic 3 – Well-defined Operations

Well-defined operations

Let's say your friend says "let's make a new operation on the rationals $\mathbb{Q}$!"

And you say "yeah we should!"

They say "What about this one?

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$$ "

new operation symbol

You say "ok let's do some calculations with this great new operation"

$$\frac{2}{7} \oplus \frac{1}{5} = \frac{2+1}{7+5} = \frac{3}{12} = \frac{1}{4}$$

$$\frac{1}{2} \oplus \frac{2}{3} = \frac{1+2}{2+3} = \frac{3}{5}$$

$$\frac{2}{3} \oplus \frac{5}{-3} = \frac{2+5}{3-3} = \frac{7}{0}$$

You're like "thats not good"

$$\frac{2}{4} \oplus \frac{20}{30} = \frac{2+20}{4+30} = \frac{22}{34} = \frac{11}{17}$$

$$\frac{2}{4} = \frac{1}{2}, \quad \frac{20}{30} = \frac{2}{3}$$

$$\frac{1}{2} \oplus \frac{2}{3} = \frac{3}{5}$$

not equal

You're like "thats really not good"

This is an example of an operation that is <u>not</u> well-defined.

Def: Let S be a set. An operation $\oplus$ on S is well-defined if the following are true:

(1) For every $x, y \in S$ we have that $x \oplus y \in S$

S is "closed" under $\oplus$

(2) If some or all of the elements of S can be expresied in more than one way, then we must show the following:

For every $a, b, c, d \in S$, if $a = b$ and $c = d$, then $a \oplus c = b \oplus d$.

Let's define two operations on the set $\mathbb{Z}_n$ ← $\boxed{\text{equivalence classes modulo } n}$

Given $\overline{x}, \overline{y} \in \mathbb{Z}_n$.

Define

$$\overline{x} + \overline{y} = \overline{x+y}$$

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Ex: Let $n=4$.

$\overline{0} = \{x \mid x \in \mathbb{Z},\ x \equiv 0 \pmod{4}\}$

$= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$

$\overline{1} = \{x \mid x \in \mathbb{Z},\ x \equiv 1 \pmod{4}\}$

$= \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

$\overline{2} = \{\ldots, -10, -6, -2, 2, 6, 10, \ldots\}$

$\overline{3} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$\overline{7} = \overline{3},\ \overline{-10} = \overline{2},\ \overline{9} = \overline{1}$ EXAMPLES

Example computations in $\mathbb{Z}_4$:

$$\overline{2} + \overline{3} = \overline{2+3} = \overline{5} = \overline{1}$$

$$\begin{array}{ccccc} \overline{2} & + & \overline{3} & & \\ \parallel & & \parallel & & \\ \overline{-10} & + & \overline{7} & = \overline{-10+7} = \overline{-3} = \overline{1} \end{array}$$

$$\begin{array}{r} 1 \\ 4\,\overline{)\,5} \\ -4 \\ \hline 1 \end{array}$$

$-3 \equiv 1 \pmod 4$

$\overline{-3} = \overline{1}$

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

$$\begin{array}{ccccc} \overline{1} & \cdot & \overline{2} & & \\ \parallel & & \parallel & & \\ \overline{9} & \cdot & \overline{6} & = \overline{9 \cdot 6} = \overline{54} = \overline{2} \end{array}$$

super-duper eq. rel. thm

$$\begin{array}{r} 13 \\ 4\,\overline{)\,54} \\ -4 \\ \hline 14 \\ -12 \\ \hline 2 \end{array}$$

<u>Theorem:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.
The following operations are well-defined on $\mathbb{Z}_n$.
Given $\bar{a}, \bar{b} \in \mathbb{Z}_n$ define

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

$\boxed{\text{proof:}}$ Let's check the two conditions to be well-defined.

<u>condition 1:</u> Given $\bar{a}, \bar{b} \in \mathbb{Z}_n$ with $a, b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$ and $a \cdot b \in \mathbb{Z}$.
So, $\overline{a+b} \in \mathbb{Z}_n$ and $\overline{a \cdot b} \in \mathbb{Z}_n$

condition 2: Suppose $a, b, c, d \in \mathbb{Z}$ and $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$ in $\mathbb{Z}_n$.

We must show that

$$\overline{a} + \overline{b} = \overline{c} + \overline{d}$$

and $\overline{a} \cdot \overline{b} = \overline{c} \cdot \overline{d}$.

Since $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$, by the super-duper equivalence class theorem we have

$a \equiv c \pmod{n}$ and

$b \equiv d \pmod{n}$.

Thus, $n \mid (a-c)$ and $n \mid (b-d)$.

So, $a-c = nk$ and $b-d = n\ell$
where $k, \ell \in \mathbb{Z}$.

Then,

$$\begin{aligned}(a+b)-(c+d) &= (a-c)+(b-d) \\ &= nk + n\ell \\ &= n(k+\ell).\end{aligned}$$

Since $k+\ell \in \mathbb{Z}$ this gives
$n \mid [(a+b)-(c+d)]$.

Thus, $(a+b) \equiv (c+d) \pmod{n}$.

Hence

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{c+d} = \overline{c} + \overline{d}$$

def of +

Also,

$$ab - cd = a\overbrace{(d+n\ell)}^{b} - \underbrace{(a-nk)}_{c}\,d$$

$$= ad + n(a\ell) - ad + n(ka)$$

$$= n(\underbrace{a\ell + ka}_{a\ell+ka \in \mathbb{Z} \text{ since } a,\ell,k\in\mathbb{Z}.})$$

So, $n \mid (ab-cd)$.

Thus, $ab \equiv cd \pmod{n}$.

Hence $\overline{a}\cdot\overline{b} = \overline{ab} = \overline{cd} = \overline{c}\cdot\overline{d}$.

def of $\cdot$

$\blacksquare$

Ex: (HW problem modified)

In $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$,

calculate $\overline{1473}$, and $\bar{5}\cdot\bar{2}+\bar{1}+\bar{2}\cdot\bar{4}\cdot\bar{6}$,

and $\overline{1455}^{10}$.

Reduce our answer to $\bar{x}$ where $0 \leq x \leq 6$.

$$\overline{1473} = \bar{3}$$

$$
\begin{array}{r}
210 \\
7\,\overline{)\,1473} \\
-14 \\
\hline
07 \\
-7 \\
\hline
03 \\
-0 \\
\hline
3
\end{array}
$$

$$\bar{5}\cdot\bar{2}+\bar{1}+\bar{2}\cdot\bar{4}\cdot\bar{6}$$

$$= \overline{10}+\bar{1}+\bar{8}\cdot\bar{6}$$

$$= \bar{3}+\bar{1}+\bar{1}\cdot\bar{6}$$

$\overline{10} = \bar{3}$

$\bar{8} = \bar{1}$

$$= \overline{4} + \overline{6}$$

$$= \overline{10} = \boxed{\overline{3}}$$

$$\begin{array}{r} 8 \\ 7\,\overline{)\,59} \\ -56 \\ \hline 3 \end{array}$$

Another way:

$$\overline{5}\cdot\overline{2} + \overline{1} + \overline{2}\cdot\overline{4}\cdot\overline{6}$$

$$= \overline{10} + \overline{1} + \overline{48}$$

$$= \overline{59} = \overline{3}$$

Another example in $\mathbb{Z}_7$

$$\begin{array}{r} 207 \\ 7\,\overline{)\,1455} \\ -14 \\ \hline 05 \\ -0 \\ \hline 55 \\ -49 \\ \hline 6 \end{array}$$

$$\overline{1455}^{10} = (\overline{6})^{10}$$

$$\overline{6} = \overline{-1}$$

$$= (\overline{-1})^{10} = \boxed{\overline{1}}$$