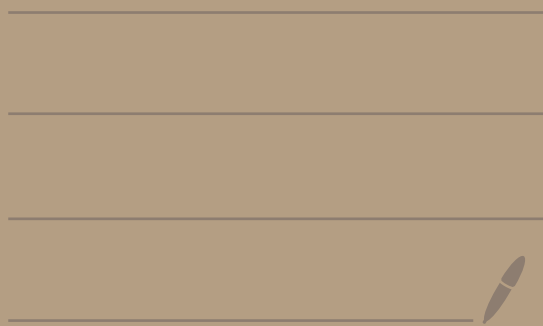


Topic 3 -  
Well-defined  
Operations

---



# 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?"

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

↑  
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  
"that's  
not good"

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

not  
equal

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

You're like  
"that's really  
not good"

This is an example of an operation that is not 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 expressed 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  $\mathbb{Z}_n$

equivalence  
classes  
modulo  $n$

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

Define

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

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

Ex: Let  $n=4$ .

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

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

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

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

$$\bar{2} = \{\dots, -10, -6, -2, 2, 6, 10, \dots\}$$

$$\bar{3} = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

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

---

$$\bar{7} = \bar{3}, \quad \bar{-10} = \bar{2}, \quad \bar{9} = \bar{1}$$

43X457X105

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

$$\begin{aligned} \overline{2} + \overline{3} &= \overline{2+3} = \overline{5} = \overline{1} \\ \parallel \quad \parallel & \\ \overline{-10} + \overline{7} &= \overline{-10+7} = \overline{-3} = \overline{1} \end{aligned}$$

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

$$\begin{aligned} \parallel \quad \parallel & \\ \overline{9} \cdot \overline{6} &= \overline{9 \cdot 6} = \overline{54} = \overline{2} \end{aligned}$$

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

$$\begin{aligned} -3 &\equiv 1 \pmod{4} \\ \overline{-3} &= \overline{1} \end{aligned}$$

Super-duper  
eq. rel. thm

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

Theorem; 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

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

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

Proof: Let's check the two conditions to be well-defined.

condition 1: 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

$\bar{a} = \bar{c}$  and  $\bar{b} = \bar{d}$  in  $\mathbb{Z}_n$ .

We must show that

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

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

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

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

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

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

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

Then,

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

Since  $k+l \in \mathbb{Z}$  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,

$$ab - cd = a \overbrace{(d + nl)}^b - \underbrace{(a - nk)}_c d$$

$$= ad + n(al) - ad + n(ka)$$

$$= n(al + ka)$$

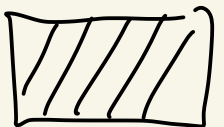
$al + ka \in \mathbb{Z}$   
since  $a, l, k \in \mathbb{Z}$ .

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

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

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

def of  $\cdot$



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  $\overline{5 \cdot 2 + 1 + 2 \cdot 4 \cdot 6}$ ,  
and  $\overline{1455}^{10}$ .

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

---

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



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

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

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

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

$$\left. \begin{array}{l} \overline{10} = \bar{3} \\ \overline{8} = \bar{1} \end{array} \right\}$$

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

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

Another way:

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

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

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

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

Another example in  $\mathbb{Z}_7$

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

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

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

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