The Integers III - Multiplication

2020-10-20

Recap: $(a,b) \sim (c,d) \iff a+d = b+c \quad (\iff a-b = c-d)$

$\mathbb{Z} = \{ [(a,b)]_\sim \mid a,b \in \mathbb{N} \} \quad ([(a,b)]_\sim = \text{"}a-b\text{"})$

Def'n: We define $[(a,b)]_\sim \cdot_\mathbb{Z} [(c,d)]_\sim$

$= [(ac+bd, ad+bc)]_\sim$.

$\big((a-b)\cdot(c-d)$

$= ac - ad - bc + bd$

$= (ac+bd) - (ad+bc) \big)$

We need to check that $\cdot_\mathbb{Z}$ is "well-defined"

ie If $[(a,b)]_\sim$ and $[(e,f)]_\sim$ are equal

and $[(c,d)]_\sim$ and $[(g,h)]_\sim$ are equal,

then $[(ac+bd, ad+bc)]_\sim = [(eg+fh, eh+fg)]_\sim$.

proof: Left as an exercise - tedious! //

Basic properties of multiplication:

1. $$[(a,b)]_\sim \cdot 0_{\mathbb{Z}} = [(a,b)]_\sim \cdot [(0,0)]_\sim = [(a0+b0,\ a0+b0)]_\sim$$
$$= [(0+0,\ 0+0)]_\sim = [(0,0)]_\sim = 0_{\mathbb{Z}}$$

2. <u>Commutativity</u>: $p \cdot_{\mathbb{Z}} q = q \cdot_{\mathbb{Z}} p$

Suppose $p = [(a,b)]_\sim$ & $q = [c,d]_\sim$. Then

$$p \cdot_{\mathbb{Z}} q = [(a,b)]_\sim \cdot_{\mathbb{Z}} [(c,d)]_\sim = [(ac+bd,\ ad+bc)]_\sim$$
$$= [(ca+db,\ da+cb)]_\sim = [(ca+db,\ cb+da)]$$
$$= [(c,d)]_\sim \cdot_{\mathbb{Z}} [(a,b)]_\sim = q \cdot_{\mathbb{Z}} p$$

$\therefore$ $\cdot_{\mathbb{Z}}$ is commutative.

3. <u>Associativity</u>: $p \cdot_{\mathbb{Z}} (q \cdot_{\mathbb{Z}} r) = (p \cdot_{\mathbb{Z}} q) \cdot_{\mathbb{Z}} r$

Suppose $p = [(a,b)]_\sim$, $q = [(c,d)]_\sim$, $r = [(e,f)]_\sim$.

(3)

Then $p \cdot_{\mathbb{Z}} (q \cdot_{\mathbb{Z}} r) = [(a,b)]_\sim \cdot_{\mathbb{Z}} \left([(c,d)]_\sim \cdot_{\mathbb{Z}} [(e,f)]_\sim \right)$

$$
\begin{aligned}
&= [(a,b)]_\sim \cdot_{\mathbb{Z}} [(ce+df,\ cf+de)]_\sim \\
&= [(a(ce+df)+b(cf+de),\ a(cf+de)+b(ce+df))]_\sim \\
&= [(ace+adf+bcf+bde,\ acf+ade+bce+bdf)]_\sim \\
&= [(ace+bde+adf+bcf,\ acf+bdf+ade+bce)]_\sim \\
&= [((ac+bd)e+(ad+bc)f,\ (ac+bd)f+(ad+bc)e)]_\sim \\
&= [(ac+bd,\ ad+bc)]_\sim \cdot_{\mathbb{Z}} [(e,f)]_\sim \\
&= \left([(a,c)]_\sim \cdot_{\mathbb{Z}} [(b,d)]_\sim \right) \cdot_{\mathbb{Z}} [(e,f)]_\sim \\
&= (p \cdot_{\mathbb{Z}} q) \cdot_{\mathbb{Z}} r
\end{aligned}
$$

$\therefore$ $\cdot_{\mathbb{Z}}$ is associative.

(4) $[(a,b)]_\sim \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = [(a,b)]_\sim \cdot_{\mathbb{Z}} [(1,0)]_\sim = [(a1+b0,\ a0+b1)]_\sim$

$$
\begin{aligned}
&= [(a+0,\ 0+b)]_\sim \\
&= [(a,b)]_\sim
\end{aligned}
$$

(5) Distributivity (of $\cdot_{\mathbb{Z}}$ over $+_{\mathbb{Z}}$):

How should this work?

Intuition:
$$\begin{cases} (a-b)\cdot\big((c-d)+(e-f)\big) \\ = (a-b)\cdot(c-d) + (a-b)\cdot(e-f) \end{cases}$$

Suppose $p = [(a,b)]_{\sim}$, $q = [(c,d)]_{\sim}$, & $r = [(e,f)]_{\sim}$.

Then $p \cdot_{\mathbb{Z}} (q +_{\mathbb{Z}} r) = [(a,b)]_{\sim} \cdot_{\mathbb{Z}} \big([(c,d)]_{\sim} +_{\mathbb{Z}} [(e,f)]_{\sim} \big)$

$$= [(a,b)] \cdot_{\mathbb{Z}} [(c+e, d+f)]_{\sim}$$
$$= [(a(c+e) + b(d+f),\ a(d+f) + b(c+e))]_{\sim}$$
$$= [(ac+ae+bd+bf,\ ad+af+bc+be)]_{\sim}$$

and $(p \cdot_{\mathbb{Z}} q) +_{\mathbb{Z}} (p \cdot_{\mathbb{Z}} r) = \big([(a,b)]_{\sim} \cdot_{\mathbb{Z}} [(c,d)]_{\sim}\big) +_{\mathbb{Z}} \big([(a,b)]_{\sim} \cdot_{\mathbb{Z}} [(e,f)]_{\sim}\big)$

$$= [(ac+bd,\ ad+bc)]_{\sim} +_{\mathbb{Z}} [(ae+bf,\ af+be)]_{\sim}$$
$$= [(ac+bd+ae+bf,\ ad+bc+af+be)]_{\sim}$$
$$= [(ac+ae+bd+bf,\ ad+af+bc+be)]_{\sim} = p \cdot_{\mathbb{Z}} (q +_{\mathbb{Z}} r)$$

$\therefore$ The Distributive Law Holds. Next time: $<$ on $\mathbb{Z}$.