The Integers II - Addition

Quick recap: We defined an equivalence relation on $\mathbb{N}\times\mathbb{N}$ by $(a,b)\sim(c,d) \iff a+d=b+c$ [idea is $a-b=c-d$].

Then the equivalence class of $(a,b)\in\mathbb{N}\times\mathbb{N}$ is $[(a,b)]_\sim = \{(c,d)\in\mathbb{N}\times\mathbb{N} \mid (a,b)\sim(c,d)\}$.

Then $(a,b)\in[(a,b)]_\sim$ and any two equivalence classes are either equal or have nothing in common.

We defined $\mathbb{Z} = \{[(a,b)]_\sim \mid (a,b)\in\mathbb{N}\times\mathbb{N}\}$.

Now we can define various specific integers and operations on $\mathbb{Z}$:

$$0_\mathbb{Z} = [(0,0)]_\sim = \{(n,n) \mid n\in\mathbb{N}\}$$

$$1_\mathbb{Z} = [(1,0)]_\sim = \{(S(n),n) \mid n\in\mathbb{N}\}$$

<u>Def'n</u>: We define $+_{\mathbb{Z}}$ on $\mathbb{Z}$ by

$$[(a,b)]_{\sim} +_{\mathbb{Z}} [(c,d)]_{\sim} = [(a+c, b+d)]_{\sim}$$

[Informally, $(a-b) +_{\mathbb{Z}} (c-d) = (a+c)-(b+d)$.]

Possible problem: Does it matter which representatives from each equivalence class we use here?

For $+_{\mathbb{Z}}$ to be "well-defined", we need to check that it doesn't matter which representatives we use from each class we use:

<u>i.e.</u> If $[(a,b)]_{\sim} = [(e,f)]_{\sim}$ (i.e. $(a,b) \sim (e,f)$)

and $[(c,d)]_{\sim} = [(g,h)]_{\sim}$ (i.e. $(c,d) \sim (g,h)$),

then $[(a+c, b+d)]_{\sim} = [(e+g, f+h)]_{\sim}$ (i.e. $(a+c, b+d) \sim (e+g, f+h)$).

This turns out to be the case:

3

Assume $(a,b)\sim(e,f)$ and $(c,d)\sim(g,h)$.

$\Rightarrow$ $a+f=b+e$ and $c+h=d+g$.

$$\Rightarrow \quad (a+f)+(c+h) = (b+e)+(d+g)$$

$$\begin{array}{lll}
\quad \| & \quad \| & \\
((a+f)+c)+h & ((b+e)+d)+g & \text{by associativity of } + \text{ in } \mathbb{N} \\
\quad \| & \quad \| & \\
(a+(f+c))+h & (b+(e+d))+g & \text{——— '' ———} \\
\quad \| & \quad \| & \\
(a+(c+f))+h & (b+(d+e))+g & \text{by commutativity of } + \text{ in } \mathbb{N} \\
\quad \| & \quad \| & \\
((a+c)+f)+h & ((b+d)+e)+g & \text{by associativity of } + \text{ in } \mathbb{N} \\
\quad \| & \quad \| & \\
(a+c)+(f+h) & (b+d)+(e+g) & \text{——— '' ———}
\end{array}$$

$\Rightarrow$ $(a+c, b+d)\sim(e+g, f+h)$ by the def'n of $\sim$

$\Rightarrow$ $[(a+c, b+d)]_\sim = [(e+g, f+h)]_\sim$ if $[(a,b)]_\sim = [(e,f)]_\sim$ & $[(c,d)]_\sim = [(g,h)]_\sim$

$\therefore$ $+_{\mathbb{Z}}$ actually is "well-defined"

Prop: For every integer $a \in \mathbb{Z}$, there is a $b \in \mathbb{Z}$ such that $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$. [We call this b, "$-a$".]

proof. Suppose $a = [(n,k)]_\sim$ for some $n, k \in \mathbb{N}$.

"$n-k$"

Let $b = [(k,n)]_\sim$.

"$-(n-k) = k-n$"

$$\text{Then } a +_{\mathbb{Z}} b = [(n,k)]_\sim +_{\mathbb{Z}} [(k,n)]_\sim = [(n+k, k+n)]_\sim \quad \text{by def'n of } +_{\mathbb{Z}}$$

$$= [(n+k, n+k)]_\sim \quad \text{by comm. of } + \text{ in } \mathbb{N}$$

$$\{(p,p) \mid p \in \mathbb{N}\} \quad = [(m,m)]_\sim \quad \text{(Check for yourself!)}$$

$$= [(0,0)]_\sim = 0_{\mathbb{Z}}.$$

//

Prop: $+_{\mathbb{Z}}$ is associative and commutative.

proof: Suppose $a = [(p,q)]_\sim$, $b = [(r,s)]_\sim$, $c = [(t,u)]_\sim$.

$$\text{Then } (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c = \left([(p,q)]_\sim + [(r,s)]_\sim\right) +_{\mathbb{Z}} [(t,u)]_\sim$$

$$= [(p+r, q+s)]_\sim +_{\mathbb{Z}} [(t,u)]_\sim$$

$$= [((p+r)+t, (q+s)+u)]_\sim = [(p+(r+t), q+(s+u))]_\sim$$

$$= [(p,q)]_\sim +_{\mathbb{Z}} [(r+t, s+u)]_\sim = [(p,q)]_\sim +_{\mathbb{Z}} \left([(r,s)]_\sim +_{\mathbb{Z}} [(t,u)]_\sim\right)$$

$$= a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c)$$

and $~~\ldots~~$ $a +_{\mathbb{Z}} b = [(p,q)]_\sim +_{\mathbb{Z}} [(r,s)]_\sim$

$$= [(p+r, q+s)]_\sim$$

$$= [(r+p, s+q)]_\sim$$

$$= [(r,s)]_\sim +_{\mathbb{Z}} [(p,q)]$$

$$= b +_{\mathbb{Z}} a .$$

$\therefore$ $+_{\mathbb{Z}}$ is both associative and commutative. //

<u>Prop:</u> $a +_{\mathbb{Z}} 0_{\mathbb{Z}} = a_{\mathbb{Z}}$ for all $a \in \mathbb{Z}$.

<u>proof:</u> If $a = [(p,q)]_\sim$, then

$$a +_{\mathbb{Z}} 0_{\mathbb{Z}} = [(p,q)]_\sim +_{\mathbb{Z}} [(0,0)]_\sim$$

$$= [(p+0, q+0)]_\sim$$

$$= [(p,q)]_\sim = a .$$

//

Next time: more $\mathbb{Z}$; $\cdot$ & $<$.