Mathematics 2200H – Mathematical Reasoning
TRENT UNIVERSITY, Fall 2024

Assignment #6
+ and · on $\mathbb{Z}$
Due on Friday, 18 October.[*]

We defined the integers, $\mathbb{Z}$, in several steps as follows. Recall that a binary relation is an equivalence relation if it is reflexive, symmetric, and transitive.

- We first defined an equivalence relation $\equiv$ on pairs of natural numbers by
$$(a,b) \equiv (c,d) \text{ if and only if } a+d=c+b.$$
Intuitively, $(a,b) \equiv (c,d)$ exactly when the two pairs represent the same difference, *i.e.* $b-a=d-c$. Note that (a,b) represents a positive difference if $a<b$, a negative difference if $b<a$, and a difference of 0 if $a=b$.
- The equivalence class of each pair of natural numbers (a,b) was defined to be the set of all pairs equivalent to the given one, that is,
$$[(a,b)]_{\equiv} = \{\, (c,d) \in \mathbb{N}\times\mathbb{N} \mid (a,b) \equiv (c,d) \,\}\,.$$
Each equivalence class groups all the pairs of natural numbers that represent the same difference.
- The integers are then officially these equivalence classes, so the set of integers is officially
$$\mathbb{Z} = \{\, [(a,b)]_{\equiv} \mid (a,b) \in \mathbb{N}\times\mathbb{N} \,\}\,.$$

We proceeded to define addition and multiplication on the official integers by
$$[(a,b)]_{\equiv} +_{\mathbb{Z}} [(c,d)]_{\equiv} = [(a+c,b+d)]_{\equiv}$$
and
$$[(a,b)]_{\equiv} \cdot_{\mathbb{Z}} [(c,d)]_{\equiv} = [(bd+ac,ad+bc)]_{\equiv}\,,$$
respectively. These operations are "well-defined", in that their definitions do not depend on the particular pairs chosen from each equivalence class. We verified this in class for addition, and you may assume that it is so for multiplication as well.

In what follows you may also assume that addition and multiplication of natural numbers have all the true algebraic properties you may need.

[*] Please submit your solutions, preferably as a single pdf, via Blackboard's Assignments module. If that fails, please submit them to the instructor on paper or via email to `sbilaniuk@trentu.ca` as soon as you can.

1. Prove that $+_{\mathbb{Z}}$ is associative and commutative. *[4]*

Solution. This is boring and tedious, but here we go, with commutativity first.

Suppose $[(a,b)]_{\equiv}, [(c,d)]_{\equiv} \in \mathbb{Z}$. Then, using the commutativity of addition on the natural numbers,

$$\begin{aligned} [(a,b)]_{\equiv} +_{\mathbb{Z}} [(c,d)]_{\equiv} &= [(a+c,b+d)]_{\equiv} \\ &= [(c+a,d+b)]_{\equiv} \\ &= [(c,d)]_{\equiv} +_{\mathbb{Z}} [(a,b)]_{\equiv} . \end{aligned}$$

Thus $+_{\mathbb{Z}}$ is commutative.

For associativity, suppose $[(a,b)]_{\equiv}, [(c,d)]_{\equiv}, [(e,f)]_{\equiv} \in \mathbb{Z}$. Then, using the associativity of addition on the natural numbers,

$$\begin{aligned} ([(a,b)]_{\equiv} +_{\mathbb{Z}} [(c,d)]_{\equiv}) +_{\mathbb{Z}} [(e,f)]_{\equiv} &= [(a+c,b+d)]_{\equiv} +_{\mathbb{Z}} [(e,f)]_{\equiv} \\ &= [((a+c)+e,(b+d)+f)]_{\equiv} \\ &= [(a+(c+e),b+(d+f))]_{\equiv} \\ &= [(a,b)]_{\equiv} +_{\mathbb{Z}} [(c+e),d+f)]_{\equiv} \\ &= [(a,b)]_{\equiv} +_{\mathbb{Z}} ([(c,d)]_{\equiv} +_{\mathbb{Z}} [(e,f)]_{\equiv}) . \end{aligned}$$

Thus $+_{\mathbb{Z}}$ is also associative. ■

2. Prove that $\cdot_{\mathbb{Z}}$ is associative and commutative. *[6]*

Solution. This is less boring, but even more tedious. Again, we'll do commutativity first.

Suppose $[(a,b)]_{\equiv}, [(c,d)]_{\equiv} \in \mathbb{Z}$. Then, using the commutativity of multiplication on the natural numbers,

$$\begin{aligned} [(a,b)]_{\equiv} \cdot_{\mathbb{Z}} [(c,d)]_{\equiv} &= [(bd+ac,ad+bc)]_{\equiv} \\ &= [(db+ca,da+bc)]_{\equiv} \\ &= [(c,d)]_{\equiv} \cdot_{\mathbb{Z}} [(a,b)]_{\equiv} . \end{aligned}$$

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

For associativity, suppose $[(a,b)]_{\equiv}, [(c,d)]_{\equiv}, [(e,f)]_{\equiv} \in \mathbb{Z}$. Then, using the associativity of multiplication on the natural numbers, plus associativity and commutativity of addition, not to mention the distributive laws for multiplication over addition,

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

Thus $\cdot_{\mathbb{Z}}$ is also associative. ■