Math Diversion Problem 858

P. Reany

October 22, 2025

And hath made of one blood all nations of men for to dwell
on all the face of the earth, and hath determined
the times before appointed, and the
bounds of their habitation;
— Acts 17:26

```
Source: The Ether of Great Mathematical Ideas
Title: Embedding a Ring into a Ring with Unity
  Presenter:  Patrick
```

1 Problem

Let R be a ring without a unity element. Show that the set S defined as follows is a ring with unity:

$$S \equiv \{(r, n) \,|\, r \in R, n \in \mathbb{Z}\}\,, \tag{1}$$

where

1) $(r, n) + (s, m) = (r + s, n + m)\,,$

2) $(r, n)(s, m) = (rs + ns + mr, nm)\,.$

Naturally, the first thing we have to do establish that S really is a ring, and that's a lot of work; and to do that, we need to figure out what it means to multiply an element of an arbitrary ring by an integer.

So, let r be an element of some arbitrary ring, then,

$$mr \equiv \underbrace{r + r + \cdots + r}_{m}\,. \tag{2}$$

So, what have we done? We have replace the operation of multiplication by an integer (which is not a natively defined operation in the ring, unless the ring is the ring of integers) with the operation of repeated addition in the ring, which is always allowed in every ring. Anyway, with the definition just given, it makes sense to insist that

$$mr = rm\,. \tag{3}$$

Also, it's clear from how we defined the addition of coordinate pairs, that addition is commutative, owing to the commutativity of addition in R and in $\mathbb{Z}$ separately.

2 What is a Ring?

This exposition is rather lengthy but can be skipped to those who know what a ring is.

Definition: A *ring* R is a set of elements on which is defined a binary operator $+$, such that:

1) For any two elements of a and b of R, $a+b=b+a$ is an element of R [binary closure under addition].

2) For any three elements of a, b, c of G, $(a+b)+c = a+(b+c)$ [addition composition associativity].

3) There exists an element 0 of R, such that for any element of r, of R, $0+r = r+0 = r$ [0 being referred to the ring's additive identity element].

4) For every element r of R, there exists an element of $-r$, of R, such that $r+(-r) = (-r)+r = 0$ [$-r$ being referred to as the element's additive inverse element in R].

Thus, we see that every ring under only addition is an additive group, and every additive group is abelian. The rules governing multiplication in a ring are similar to those governing a group, except that ring elements do not necessarily have multiplicative inverses for each ring element. The ring of integers is like that. For example, its element 5 does not have a multiplicative inverse in the integers. The next ring up from the integers that contains multiplicative inverses for all its elements is the ring of rational numbers $(\mathbb{Q}, +, \cdot)$. And, of course, we are free to drop the $\cdot$ for multiplication in an expression, so long as the resulting expression is unambiguous.

Proceeding along, the rules governing ring multiplication are as follows:

1) For any two elements of a and b of R, ab and ba are elements of R [binary closure under multiplication].

2) For any three elements of a, b, c of R, $(ab)c = a(bc)$ [multiplicative composition associativity].

3) For any three elements of a, b, c of R, $a(b+c) = ab+ac$ [left multiplicative distributivity over addition].

4) For any three elements of a, b, c of R, $(b+c)a = ba+ca$ [right multiplicative distributivity over addition].

So, what about the existence of a multiplicative identity element in a ring? For the moment, lets use the symbol "1" to refer to the multiplicative identity element of a ring R, if the ring even has one. Then for every element r of R, $1r = r1 = r$.

The ring axioms listed for convenience:

For all $a, b, c \in R$,

a) $a + b = b + a$ for all $a, b \in R$

There exists a $0 \in R$ such that for all $a \in R$
b) $a + 0 = 0 + a = a$

For all $a, b, c \in R$
c) $(a + b) + c = a + (b + c)$
d) $(ab)c = a(bc)$
e) $c(a + b) = ca + cb$
f) $(a + b)c = ac + bc$

If R is unital (i.e., has a unitary element, say '1') then for all $a \in R$:
g) $1a = a1 = a$

Definition: If every pair of elements of a given ring commute under multiplication the ring is said to be **commutative**. There are plenty of rings that are not commutative. The ring of $n \times n$ matrices over the reals for $n \geq 2$ are not commutative.

3 Proof

If S is to be a ring, it must have a zero element. The likely candidate for that is $(0, 0)$. Let's prove this:

$$(0, 0) + (r, n) = (0 + r, 0 + n) = (r, n)\,, \tag{4}$$

And since we've already shown that addition is commutative in S, we are finished. I'll leave it to the interested reader to prove that addition in S is associative. This is obvious because the components inherit associativity under addition from that in R and in $\mathbb{Z}$.

So, we are assuming that the integers play the role of scalars in that they commute not only with each other, but also with all the elements of R.

Next, what might be the unity element in S? How about $(0, 1)$? So, let's prove it, if so. By the way, how shall we interpret '$1 \cdot r$' for $r \in R$? We interpret it as adding one r's together, hence

$$1 \cdot r = r \cdot 1 = r\,. \tag{5}$$

Now,

$$(0,1)(s,m) = (0 \cdot s + 1 \cdot s + 0 \cdot m, 1 \cdot m) = (s,m)$$
$$(r,n)(0,1) = (r \cdot 0 + n \cdot 0 + 1 \cdot r, n \cdot 1) = (r,n)\,. \tag{6}$$

I won't take the time to show that this unity element is unique in S.

Next, we need to show that multiplication in S distributes over addition.

Left distributivity:

We need to show that

$$(R,N)[(r,n) + (s,m)] = (R,N)(r,n) + (R,N)(s,m)\,. \tag{7}$$

We'll do the LHS and the RHS separately, starting with the LHS. (But before we do, we need to remember that we have not assumed that R is a commutative ring, hence, we cannot assume that $rs = sr$ for all r, s in R.)

$$\begin{aligned}(R,N)[(r,n) + (s,m)] &= (R,N)(r+s, n+m) \\ &= (R(r+s) + N(r+s) + R(n+m), N(n+m))\,.\end{aligned} \tag{8}$$

Now, for the RHS:

$$\begin{aligned}(R,N)(r,n) + (R,N)(s,m) &= (Rr + Nr + Rn, Nn) + (Rs + Ns + Rm, Nm) \\ &= (R(r+s) + N(r+s) + R(n+m), N(n+m))\,.\end{aligned} \tag{9}$$

Since, the LHS side is equal to the RHS, we've shown that left distributivity holds in S.

I leave it as an exercise to show that right distributivity also holds in S.

Next, we establish that multiplication in S is associative, which will get messy. We need to show that for arbitrary elements $R, S, T \in R$, and arbitrary integers N, M, P that

$$(R,N)[(S,M)(T,P)] = [(R,N)(S,M)](T,P)\,. \tag{10}$$

I repeat the rule for multiplication of pairs:

$$(r,n)(s,m) = (rs + ns + mr, nm) \tag{11}$$

So, let's get to it.

$$\begin{aligned}(R,N)[(S,M)(T,P)] &= (R,N)(ST + MT + PS, MP) \\ &= \big(R(ST + MT + SP) + N(ST + MT + PS) \\ &\qquad + MPR, NMP\big) \\ &= (RST + MRT + PRS + NST + NMT \\ &\qquad + NPS + PMR, NMP)\,.\end{aligned} \tag{12}$$

Next, we expand the RHS of (10):

$$
\begin{aligned}
[(R, N)(S, M)](T, P) &= (RS + NS + MR, NM)(T, P) \\
&= \big(RST + NST + MRT + NMT \\
&\qquad + P(RS + NS + MR), NMP\big) \\
&= \big(RST + NST + MRT + NMT \\
&\qquad + PRS + PNS + PMR), NMP\big)\,. \qquad (13)
\end{aligned}
$$

Since the RHS's of (12) and (13) are equal, we have shown that multiplication in S is associative.