Errata 1

Math 351

March 24, 2016

Here is our definition of unit of a not [necessarily commutative] ring:

Definition. An element a in a ring R is a *unit* if there exists $b \in R$ such that $ab = ba = 1$.

When defining it in class, I've made a comment that it suffices to ask that $ab = 1$, and we would get that $ba = 1$ also. This is *incorrect*! It does work in the context of groups, but not rings in general.

Here is something that we do have:

Proposition. *Let R be a ring and $a \in R$ such that there are $b, c \in R$ such that $ab = ca = 1$. [So, b is a "left inverse" and c is a "right inverse".] Then, $b = c$. [So, if a has both a right and left inverses, these must be the same.]*

Proof. This is simple. We have:

$$b = 1 \cdot b = (ca) \cdot b = c \cdot (ab) = c \cdot 1 = c.$$

$\square$

Here is the result that actually works [and lead to my mistake]:

Proposition. *Let $R \neq \{0\}$ be a ring such that for* every *$a \in R \setminus \{0\}$ there is $b \in R$ such that $ba = 1$. [I.e.,* every *element has a left inverse.] Then, $ab = 1$. [I.e., the left inverse is also a right inverse.]*

Proof. First, observe that $ab \neq 0$, as otherwise we would get that

$$0 = b \cdot 0 = b(ab) = (ba)b = 1 \cdot b = b.$$

But then, $1 = ba = 0 \cdot a = 0$, a contradiction since $R \neq \{0\}$. Hence, $ab \neq 0$.

Now, since $ab \neq 0$, we have it has a left inverse [by hypothesis]. Let then c be a left inverse of ab. Then, $c(ab) = cab = 1$ and hence $caba = a$. But, since $ba = 1$, we get $ca = ca \cdot 1 = caba = a$. But then, $ab = cab = 1$. [The first equality follows from $a = ca$ and the second from $cab = 1$.] □

But, indeed, a [non-commutative] ring can have a left inverse which is not a right inverse:

Example: Let

$$S \stackrel{\text{def}}{=} \{\{a_i\} = (a_0, a_1, a_2, \dots) : a_i \in \mathbb{R}\},$$

i.e., the set of real sequences. Define:

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) \stackrel{\text{def}}{=} (a_0 + b_0, a_1 + b_1, \dots).$$

[I.e., we add two sequences by adding the corresponding terms.]
Now, let

$$R \stackrel{\text{def}}{=} \{f \mid f : S \to S\}$$

[i.e., the set of all functions from S to S]. To make R into a ring we need two operations. Define $f + g$ in the usual way:

$$(f + g)(\{a_i\}) \stackrel{\text{def}}{=} f(\{a_i\}) + g(\{a_i\}).$$

For the product, though, we will use *composition of functions* [and *not* multiplication of sequences by multiplying the corresponding entries, and so R is *not* the ring $\mathcal{F}(S, S)$ that I previously defined in class!]. Thus,

$$(f \cdot g)(\{a_i\}) \stackrel{\text{def}}{=} (f \circ g)(\{a_i\}) = f(g(\{a_i\})).$$

Check that these operation do make R into a [non-commutative] ring [with 1]. [Note that 0_R is the function that takes every sequence to $(0, 0, 0, \dots)$ and 1_R is the identity function [that takes every sequence to itself].]
Let now $f \in R$ be defined by:

$$f((a_0, a_1, a_2, \dots)) \stackrel{\text{def}}{=} (0, a_0, a_1, a_2, \dots),$$

[i.e., f adds a 0 to the first entry and shifts the rest up] and $g \in R$ be defined by:

$$g((a_0, a_1, a_2, \dots)) \stackrel{\text{def}}{=} (a_1, a_2, a_3, \dots)$$

[i.e., g removes the first entry, shifting the rest down]. Then,

$$(g \cdot f)((a_0, a_1, a_2, \ldots)) = g(f((a_0, a_1, a_2, \ldots))) = g((0, a_0, a_1, a_2, \ldots) = (a_0, a_1, a_2, \ldots),$$

i.e., $g \cdot f = 1_R$.
But,

$$(f \cdot g)((1, 0, 0, 0, \ldots)) = f(g(1, 0, 0, 0, \ldots)) = f((0, 0, 0, \ldots)) = (0, 0, 0, 0, \ldots) \neq (1, 0, 0, 0, \ldots),$$

and hence $f \cdot g \neq 1_R$. So, g is a left inverse of f in R, but *not* a right inverse [and f is a ring inverse of g, but not a left inverse].