MTH4104 **Introduction to Algebra**

Week 6 tutorial questions **w/c 28 February 2022**

This sheet contains questions for you to work through in your tutorial, singly or in a group.

It's important to work through lots of questions for practice. Remember that mathematics is not a spectator sport! If you want more questions, look at the "Extra questions" sheets on QMPlus.

Question 1 Give an example of a ring R and an element $a \in R$ such that $a \neq 0$ but $a^2 = 0$ in R.

Solution An example is that in $R = \mathbb{Z}_4$, the element $a = [2]_4$ is nonzero, but $a^2 = [4]_4 = [0]_4$ is zero.

Question 2 Let R be the subset $\{[2a]_6 : a \in \mathbb{Z}\} = \{[0]_6, [2]_6, [4]_6\}$ of $\mathbb{Z}_6$. Endow R with the same definitions of addition and multiplication used for $\mathbb{Z}_6$.

(a) Does R satisfy the identity law for multiplication? Justify your answer.

(b) Is R a ring? Is R a field?

Solution (a) R does satisfy the identity law for multiplication, with $[4]_6$ as the multiplicative identity element. Since R is finite, this can be checked by brute force. Alternatively, any element of R can be written in the form $[2a]_6$, and multiplying by $[4]_6$ gives

$$[4]_6 \cdot [2a]_6 = [8a]_6 = [2a]_6,$$

the second equation being true because $8a - 2a$ is a multiple of 6. (Since multiplication in $\mathbb{Z}_6$ is commutative, $[2a]_6 \cdot [4]_6 = [2a]_6$ as well.)

The point of this question is that $[1]_6 \notin R$. If $R \subseteq S$ and S is a ring, just because 1_S is not an element of R doesn't mean the multiplicative identity law is false for R. The identity element can change, even if the definition of multiplication does not change. So watch out for this subtlety when you're working with subsets of a ring.

(Note that if a subset of a ring is also a ring with the same definition of addition, the additive identity element *cannot* change. See if you can figure out why, and how multiplication is different.)

(b) R is a field, and therefore it is also a ring.

I will give a quick justification. The associative, commutative, and distributive laws are true for R because they are true for $\mathbb{Z}_6$. Both closure laws are true: given $[2a]_6$ and $[2b]_6$ in R, their sum $[2(a+b)]_6$ and product $[4ab]_6$ are congruence classes of even numbers and therefore in R. $[0]_6 \in R$ is still the additive identity element, for the same reason as in $\mathbb{Z}_6$. We showed above that $[4]_6$ is the multiplicative identity element; since $[4]_6 \neq [0]_6$, the nontrivial law is true. The additive inverse law holds because the additive inverse of $[2a]_6 \in R$ is still $[2(-a)]_6 \in R$. Finally, the only nonzero elements of R are $[2]_6$ and $[4]_6$, and you can check that each of these has square $[4]_6$, so it is its own multiplicative inverse in R: therefore, the multiplicative inverse law is true.

Question 3 Let m be a positive integer.

(a) Write up a careful proof of the associative law for addition for $\mathbb{Z}_m$.

(b) Your proof in part (a) probably comes down to the associative law for addition for $\mathbb{Z}$, together with "taking care of the brackets" $[\cdots]_m$.

Of all the axioms for a commutative ring with identity, which of them can be proved for $\mathbb{Z}_m$ in a similar way?

Solution (a) We must show that, given any three elements $x,y,z \in \mathbb{Z}_m$, the equation $(x+y)+z = x+(y+z)$ holds. To use the definition of addition in $\mathbb{Z}_m$, we need to choose representatives from the congruence classes: let $x = [a]_m$, $y = [b]_m$, and $z = [c]_m$ for integers a, b, and c. Then, using that definition,

$$(x+y)+z = ([a]_m + [b]_m) + [c]_m = [a+b]_m + [c]_m = [(a+b)+c]_m$$

while

$$x+(y+z) = [a]_m + ([b]_m + [c]_m) = [a]_m + [b+c]_m = [a+(b+c)]_m$$

which are equal, because of course $(a+b)+c = a+(b+c)$ as integers. This proves the associative law for addition.

(b) I wrote my proof in part (a) a little pedantically, with parentheses in $(a+b)+c$ and $a+(b+c)$ which you probably left out, to show that the associative law in the integers is in play.

As you can see, once we pick a representative for each congruence class, using the definitions to simplify $(x+y)+z$ turns it to $[(a+b)+c]_m$, thus "moving the $[\ ]_m$ to the outside". The same will happen for any expression built from the variables using $+$ and $\cdot$. So for any axiom which says

$$\text{"for any elements } x,y,\ldots \in \mathbb{Z}_m, \text{ (some expression)} = \text{(another expression)"}, \qquad (1)$$

moving the $[\ ]_m$ to the outside will leave the same expressions inside but with the variables being integers. Then we can finish the proof using the axiom in question for the integers.

Both associative laws, both commutative laws, and the distributive law are of the form (1), so they have proofs like part (a). For the identity laws we need to pick identity elements; but if we pick $[0]_m$ and $[1]_m$, then we get 0 and 1 inside after we move the $[\,]_m$ to the outside, so they have proofs like part (a) as well. For the additive inverse law we need to specify a way to find the additive inverse (i.e. negative) of a congruence class; once we pick $-[a]_m = [-a]_m$, then this proof falls in line too. And that's everything but the closure laws.

As I've said in lecture, the closure laws are in the list mostly to remind you to check that your addition and multiplication operators are well-defined and their codomain really is the set R. We have already checked this for modular arithmetic quite thoroughly, but these well-definedness checks are unlike anything we encountered when just thinking of $\mathbb{Z}$.

Question 4 Let R be a ring. Prove carefully that

$$(-a)b = -(ab) = a(-b)$$

for any elements $a, b \in R$. Name the ring axiom or proposition you are using at each step of your argument.

Solution You might be tempted to write (e.g.) $-a$ as $-1 \cdot a$ and then take advantage of the associative law. But since R might not be a ring with identity, it need not have an element -1. So we must take a different approach.

Let us first prove the equation $-(ab) = (-a)b$. The defining property of the element $-a$, given by the additive inverse law, is

$$a + (-a) = 0.$$

Multiplying by b yields

$$\begin{aligned} 0 &= 0b && \text{(Proposition 3.13)} \\ &= (a + (-a))b && \text{(additive inverse)} \\ &= ab + (-a)b && \text{(distributive)} \end{aligned}$$

using distributivity and our lemma about multiplication by 0. Since $ab + (-a)b = 0$ (and by commutativity $(-a)b + ab = 0$), we see that $(-a)b$ is the additive inverse of ab, that is, $(-a)b = -(ab)$.

It remains to prove the equation $-(ab) = a(-b)$. This proof is just like the above one reflected left to right, as it were, so I will be less fastidious about naming the laws. The additive inverse and distributive laws, and Proposition 3.13 about multiplication by 0, imply

$$0 = a0 = a(b + (-b)) = ab + a(-b).$$

Hence, by the definition of the inverse, we conclude $-ab = a(-b)$.