Queen Mary University of London

MTH4104 **Introduction to Algebra**

Week 8 tutorial questions **w/c 14 March 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 Let $f = [2]_8 x + [3]_8$ and $g = [4]_8 x^2 + [6]_8 x + [3]_8$ be elements of $\mathbb{Z}_8[x]$. Compute the sum $f+g$ and product fg.

Solution I've worked out $f+g$ below. To use the definition I first rewrite $f = [0]_8 x^2 + [2]_8 x + [3]_8$ so that f and g have the same number of terms. Then, by definition,

$$\begin{aligned} f+g &= ([0]_8 + [4]_8)x^2 + ([2]_8 + [6]_8)x + ([3]_8 + [3]_8) \\ &= [4]_8 x^2 + [8]_8 x + [6]_8 \\ &= [4]_8 x^2 + [0]_8 x + [6]_8 \end{aligned}$$

which I can if I like also write as $[4]_8 x^2 + [6]_8$, since $[0]_8$ is the additive identity element (i.e. the 0) of $\mathbb{Z}_8$.

Next, here is fg. The first line uses the definition of multiplication in $\mathbb{Z}_8[x]$; the rest is doing sums and products in $\mathbb{Z}_8$ to work out the coefficients.

$$\begin{aligned} fg &= ([2]_8[4]_8)x^3 + ([2]_8[6]_8 + [3]_8[4]_8)x^2 + ([2]_8[3]_8 + [3]_8[6]_8)x + [3]_8[3]_8 \\ &= [2\cdot 4]_8 x^3 + [2\cdot 6 + 3\cdot 4]_8 x^2 + [2\cdot 3 + 3\cdot 6]_8 x + [3\cdot 3]_8 \\ &= [8]_8 x^3 + [24]_8 x^2 + [24]_8 x + [9]_8 \\ &= [0]_8 x^3 + [0]_8 x^2 + [0]_8 x + [1]_8 \\ &= [1]_8. \end{aligned}$$

In other words, f and g are multiplicative inverses of each other in $\mathbb{Z}_8[x]$! This illustrates a difference between the behaviour of $R[x]$ when R is a field (or a skewfield) and when it isn't. Non-constant polynomials never have multiplicative inverses in $R[x]$ when R is a skewfield, as you probably know at least when $R = \mathbb{R}$.

Question 2 Let R be a skewfield. Let f and g be nonzero polynomials in $R[x]$, of degrees m and n, respectively.

(a) Is $\deg(fg)$ uniquely determined by this information? If so, what is it? If not, what are the possible values it can take?

(b) The same questions for $\deg(f+g)$.

Solution (a) When $R=\mathbb{R}$, your experience with real polynomials should tell you that $\deg(fg)$ must equal $m+n$. This is in fact the correct answer when R is any skewfield, but there is a potential gotcha: did you notice it?

By the assumption on their degrees, f and g can be written out as

$$f = a_m x^m + \cdots + a_1 x + a_0,$$
$$g = b_n x^n + \cdots + b_1 x + b_0$$

where $a_0,\ldots,a_m$ and $b_0,\ldots,b_n$ are elements of R with $a_m \neq 0$ and $b_n \neq 0$. Our formula for the product says

$$fg = a_m b_n x^{m+n} + (a_m b_{n-1} + a_{m-1} b_n) x^{m+n-1} + \cdots$$

which certainly looks like it has degree $m+n$. But to be sure of this, we need to check that the coefficient $a_m b_n$ is not zero!

Suppose, for a contradiction, that $a_m b_n = 0$. We have assumed $a_m \neq 0$, and since R is a skewfield, a_m has a multiplicative inverse a_m^{-1}. Multiplying $0 = a_m b_n$ on the left by a_m^{-1}, we get

$$0 = a_m^{-1} 0 = a_m^{-1}(a_m b_n) = (a_m^{-1} a_m) b_n = 1 b_n = b_n,$$

but this is a contradiction since we assumed that $b_m \neq 0$ also. We have therefore proved that $a_m b_n \neq 0$, and therefore $\deg(fg) = m+n$.

(b) The degree of $f+g$ must be equal to $\max(m,n)$ unless $m=n$, in which case the degree of $f+g$ could also be any smaller natural number, or undefined.

To briefly explain, the exponents appearing in terms of $f+g$ are those which appear in f or in g, except that an exponent which appears in both f and g could fail to appear in $f+g$ because the coefficients cancel, i.e. f has a term ax^i and g has the term $-ax^i$. These cancellations will not affect the degree unless they occur in the leading term of both f and g, which is only possible if $m=n$. If this happens, cancellations could take place in any number of the smaller terms as well.

Question 3 In lectures I didn't prove that $R[x]$ was a ring. This question is to get you to try filling in a piece of that proof.

Let R be a ring. Prove the left distributive law for $R[x]$.

Solution Let A, B, and C be three elements of $R[x]$. We may write them out, using sigma notation to be concise, as $A = \sum_{i=0}^{m} a_i x^i$, $B = \sum_{i=0}^{n} b_i x^i$, and $C = \sum_{i=0}^{n} c_i x^i$, where the a_i, b_i, and c_i are elements of R. Note that I have taken the same upper bound, n, in the sums for B and C. I can do this: if their degrees are actually different, I can append

terms with zero coefficients to the front of whichever one has lesser degree. I've done so only for convenience when I write out the sum.

We must evaluate $A(B+C)$ and $AB+AC$, and compare them. Now $B+C = \sum_{i=0}^{n}(b_i+c_i)x^i$, whence

$$A(B+C) = \sum_{i=0}^{m+n}\left(\sum_{j+k=i} a_j(b_k+c_k)\right)x^i.$$

On the other hand the sum of

$$AB = \sum_{i=0}^{m+n}\left(\sum_{j+k=i} a_j b_k\right)x^i$$

and

$$AC = \sum_{i=0}^{m+n}\left(\sum_{j+k=i} a_j c_k\right)x^i$$

is

$$AB+AC = \sum_{i=0}^{m+n}\left(\sum_{j+k=i} a_j b_k\right) + \left(\sum_{j+k=i} a_j c_k\right)x^i.$$

So what is left to do is show that corresponding coefficients of these two polynomials are equal, namely, that

$$\sum_{j+k=i} a_j(b_k+c_k) = \Big(\sum_{j+k=i} a_j b_k\Big) + \Big(\sum_{j+k=i} a_j c_k\Big)$$

This is true by the ring axioms in R. First, using distributivity on each summand of the sum on the left hand side shows that it equals

$$\sum_{j+k=i} a_j b_k + a_j c_k.$$

Now, a succession of uses of the associative and commutative laws for addition (the former to move around the parentheses that I haven't written) lets us separate the $a_j b_k$ terms from the $a_j c_k$ terms, showing this is equal to

$$\sum_{j+k=i} a_j b_k + \sum_{j+k=i} a_j c_k,$$

the expression on the right hand side.

Question 4 Recall from section 4.1 of the notes that, for any ring R, each polynomial $f \in R[x]$ determines a function $R \to R$, which we usually also call f.

Give an example of a non-commutative ring R, two polynomials $f, g \in R[x]$, and an element $r \in R$ such that $(fg)(r) \neq f(r)\cdot g(r)$.

[To answer this question, of course, you must know an example of a non-commutative ring. If you don't yet know any, come back to this question in a fortnight, after we have studied matrices.]

Solution Since R is a non-commutative ring, there exist elements $u, v \in R$ such that $uv \neq vu$. What we need to do for this question is to figure out where to put those u and v into f, g, and r to arrange that $(fg)(r) \neq f(r) \cdot g(r)$.

To make it easy, let's try to use the simplest polynomials we can. Making f and g constant polynomials won't work, since the r wouldn't actually show up and we'd just be multiplying the same two elements of R on both sides. So let's try linear polynomials, $f = ax + b$ and $g = cx + d$. Using the definition of multiplication in $R[x]$,

$$fg = acx^2 + (ad + bc)x + bd$$

so $(fg)(r) = acr^2 + (ad + bc)r + bd$. On the other hand, using distributivity in R,

$$\begin{aligned} f(r) \cdot g(r) &= (ar + b) \cdot (cr + d) \\ &= ar(cr + d) + b(cr + d) \\ &= arcr + ard + bcr + bd. \end{aligned}$$

So there are two mismatches between these results: in $(fg)(r)$ we have terms acr^2 and adr, but in $f(r) \cdot g(r)$ we have terms $arcr$ and ard. We could exploit either of these mismatches for our counterexample. Let's pick the latter one and try to make $adr \neq ard$. Using our assumption $uv \neq vu$, we can do this if we put $r = u$, $d = v$, and $a = \ldots$ well, the easiest way not to cause trouble with a is to take $a = 1$, so let's assume R is a ring with identity. Then if we set $b = c = 0$, the other terms will all be zero and not interfere with the relevant inequality. The conclusion is that

$$f = x, \quad g = v, \quad r = u$$

is a counterexample, where g is a constant polynomial.

Here's that counterexample in an actual ring, the ring $R = \mathrm{M}_2(\mathbb{R})$ of 2×2 real matrices. From the notes, a pair of matrices in R that don't commute are $u = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $v = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Using these, our counterexample is

$$f = x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad g = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad r = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Question 5 Give an example of a finite ring R and a function $f : R \to R$ that is not a polynomial function, in the sense of section 4.1 of the notes. Justify your answer.

Solution You know lots of functions from $\mathbb{R}$ to $\mathbb{R}$ that are not polynomial, like the exponential function $\exp : \mathbb{R} \to \mathbb{R}$, $\exp(x) = e^x$, or the function $g : \mathbb{R} \to \mathbb{R}$ given by

$$g(x) = \begin{cases} 1/x & x \neq 0 \\ \text{[any constant you like]} & x = 0 \end{cases}$$

where the second case is there just to make g a well-defined total function, or for that matter even

$$\delta(x) = \begin{cases} 0 & x \neq 0 \\ 1 & x = 0 \end{cases}$$

since polynomial functions on $\mathbb{R}$ are continuous but δ is not.

Over finite rings, this is harder. You might try to set up an example in a finite ring based on one of the above real examples, and then discover that it is in fact a polynomial, given by some formula different than the one you thought of. It turns out that, when R is a finite *field*, every function $R \to R$ is a polynomial function. For example, when $R = \mathbb{Z}_p$ for a prime number p, Fermat's little theorem implies that the analogue of δ above is the polynomial function

$$[-1]_p x^{p-1} + [1]_p = \begin{cases} 0 & x \neq 0 \\ 1 & x = 0. \end{cases}$$

Since a field won't work, let's try $\mathbb{Z}_m$ where m is not a prime, say $m = 4$. Given any polynomial

$$p = p_n x^n + \cdots + p_1 x + p_0 \in \mathbb{Z}_4[x],$$

let $p_i = [a_i]_4$ for an integer a_i. Then we can make a table of values of the function p:

$b \in \mathbb{Z}_4$	$p(b)$
$[0]_4$	$p_n[0]_4^n + \cdots + p_1[0]_4 + p_0 = [a_n \cdot 0^n + \cdots + a_1 \cdot 0 + a_0]_4$
$[1]_4$	$p_n[1]_4^n + \cdots + p_1[1]_4 + p_0 = [a_n \cdot 1^n + \cdots + a_1 \cdot 1 + a_0]_4$
$[2]_4$	$p_n[2]_4^n + \cdots + p_1[2]_4 + p_0 = [a_n \cdot 2^n + \cdots + a_1 \cdot 2 + a_0]_4$
$[3]_4$	$p_n[3]_4^n + \cdots + p_1[3]_4 + p_0 = [a_n \cdot 3^n + \cdots + a_1 \cdot 3 + a_0]_4$

Now the question is: how can we make a list of 4 elements of $\mathbb{Z}_4$ which is not equal to the list in this table for any $a_n, \ldots, a_1, a_0 \in \mathbb{Z}$? Here's one way.

The key fact used in this example is that each congruence class in $\mathbb{Z}_4$ contains either even integers only or odd integers only. The integer $a_n \cdot 2^n + \cdots + a_1 \cdot 2 + a_0$, from the $[2]_4$ row of the table is even if a_0 is even, and odd if a_0 is odd. But the integer in the $[0]_4$ row of the table is itself just $a_n \cdot 2^n + \cdots + a_1 \cdot 2 + a_0 = a_0$. That is, $p([0]_4)$ and $p([2]_4)$ are either both congruence classes of even numbers or both congruence classes of odd numbers, no matter what p is. Therefore,

$$\delta(x) = \begin{cases} [0]_4 & x \neq [0]_4 \\ [1]_4 & x = [0]_4 \end{cases}$$

is one example of a function $\delta : \mathbb{Z}_4 \to \mathbb{Z}_4$ that is not a polynomial function, because $\delta([0]_4) = [1]_4$ is the congruence class of an even number because $\delta([2]_4) = [0]_4$ is the congruence class of an odd number.