Queen Mary University of London

**MTH4104** **Introduction to Algebra**

**Week 9 tutorial questions** **w/c 21 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** What are the quotient and remainder when $x^5$ is divided by $x^2+(1+\mathrm{i})x+\mathrm{i}$ in $\mathbb{C}[x]$?

**Solution** We can compute this by long division.

$$
\begin{array}{rl}
 & x^3+(-1-\mathrm{i})x^2+\mathrm{i}x+0 \\
\cline{2-2}
x^2+(1+\mathrm{i})x+\mathrm{i} \;\big)\; x^5 & \\
x^5+(1+\mathrm{i})x^4+\mathrm{i}x^3 & \\
\cline{1-1}
(-1-\mathrm{i})x^4-\mathrm{i}x^3 & \\
(-1-\mathrm{i})x^4-2\mathrm{i}x^3+(1-\mathrm{i})x^2 & \\
\cline{1-1}
\mathrm{i}x^3+(-1+\mathrm{i})x^2 & \\
\mathrm{i}x^3+(-1+\mathrm{i})x^2-x & \\
\cline{1-1}
0x^2+x & \\
0x^2 & \\
\cline{1-1}
x &
\end{array}
$$

So the quotient is $x^3+(-1-\mathrm{i})x^2+\mathrm{i}x$ and the remainder is $x$.

**Question 2** Let $R$ be the relation on the set $\mathbb{R}[x]$ defined by

$$f R g \text{ if and only if } x^2+1 \text{ divides } g-f$$

for all $f,g\in\mathbb{R}[x]$.

(a) Prove that $R$ is an equivalence relation.

(b) Prove that, in every equivalence class of $R$, there is exactly one polynomial $h$ such that $h=0$ or $\deg h\leq 1$.

(c) Let $f,g\in\mathbb{R}[x]$ be polynomials such that $fRg$. Prove that $f(\mathrm{i})=g(\mathrm{i})$ as complex numbers. From this point of view, what is special about the polynomial $h$ from part (b)?

**Solution** (a) We must show that $R$ is reflexive, symmetric, and transitive.

**Reflexivity** Let $f \in \mathbb{R}[x]$. In $\mathbb{R}[x]$ we have $0 = 0(x^2+1)$, so $x^2+1$ divides $0 = f - f$, implying $fRf$.

**Symmetry** Suppose $f, g \in \mathbb{R}[x]$ satisfy $fRg$, so $g - f = k(x^2+1)$ for some $k \in \mathbb{R}[x]$. Then $f - g = (-k)(x^2+1)$, implying $gRf$.

**Transitivity** Suppose $f, g, h \in \mathbb{R}[x]$ satisfy $fRg$ and $gRh$. This means there exist $k, l \in \mathbb{R}[x]$ such that $g - f = k(x^2+1)$ and $h - g = l(x^2+1)$. Then

$$h - f = (h-g) + (g-f) = (k+l)(x^2-1)$$

implying $fRh$.

(b) Let $f \in \mathbb{R}[x]$. We must show existence and uniqueness of a polynomial $h \in [f]_R$ of degree $\leq 1$ (allowing this to include the zero polynomial for convenience).

**Existence** Let $r$ be the remainder on division of $f$ by $x^2+1$, so that $f = q(x^2+1) + r$ where $q$ is the quotient. Then $x^2+1$ divides $f - r = q(x^2+1)$, so $r \in [f]_R$.

**Uniqueness** Suppose $ax+b, a'x+b'$ are distinct polynomials in $[f]_R$ of degree $\leq 1$. Then $x^2+1$ divides $(ax+b) - (a'x+b') = (a-a')x + (b-b')$. By assumption this difference is nonzero. However, by coursework, any nonzero multiple of $x^2+1$ has degree greater than or equal to $\deg(x^2+1) = 2$, while $(a-a')x + (b-b')$ has degree at most 1, a contradiction.

(c) Let $f, g \in \mathbb{R}[x]$ satisfy $fRg$. By the definition of divisibility, there is a polynomial $k \in \mathbb{R}[x]$ such that

$$g - f = k \cdot (x^2+1).$$

Now interpret all of these polynomials as elements of $\mathbb{C}[x]$, and evaluate both sides of the above equation at $x = \mathrm{i}$. We get

$$g(\mathrm{i}) - f(\mathrm{i}) = k(\mathrm{i}) \cdot (\mathrm{i}^2+1) = k(\mathrm{i}) \cdot 0 = 0.$$

Therefore $f(\mathrm{i}) = g(\mathrm{i})$.

If $f \in \mathbb{R}[x]$ is some polynomial and $h = a + bx \in [f]_R$ is the polynomial found in part (b) – apologies for the switch in notation for the coefficients! – then $f(\mathrm{i}) = h(\mathrm{i}) = a + b\mathrm{i}$. But every complex number can be written uniquely in the standard form $a + b\mathrm{i}$, where $a$ and $b$ are real numbers. So the special thing about $h$ is that it provides the standard form of the complex value $f(\mathrm{i})$ shared by all the polynomials $f$ in its equivalence class.

## Question 3

(a) Give an example of a ring $R$ and a polynomial $f \in R[x]$ such that the number of solutions $\alpha \in R$ to $f(\alpha) = 0$ is greater than $\deg f$.

[Hint: I've shown you one in lectures in a different context.]

(b) If the proofs in Sections 4.3 and 4.5 of the lecture notes were applicable to your ring $R$ from part (a), they would imply that $f(\alpha) = 0$ could have at most $\deg f$ solutions. If you try to apply these proofs to $R$, where do they go wrong?

**Solution** (a) The example I showed in lectures was that for the degree 2 polynomial $x^2 - x \in \mathbb{Z}_6[x]$ (or to be fully explicit, $[1]_6 x^2 + [-1]_6 x + [0]_6$) there are four zeroes in $\mathbb{Z}_6$, namely $[0]_6, [1]_6, [3]_6, [4]_6$. I did this example when talking about solving equations in $\mathbb{Z}_m$ by trial and error.

There are many other examples. For example, the zeroes of the matrix polynomial $x^2 \in \mathrm{M}_2(\mathbb{R})[x]$ are $2 \times 2$ real matrices whose square is zero, and there are infinitely many of these. Any conjugate of the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ has square zero, and this includes e.g. all matrices of the form $\begin{pmatrix} ar & a \\ -ar^2 & -ar \end{pmatrix}$ for $a, r \in \mathbb{R}$.

(b) The explanation depends on what your example from part (a) was.

If $R$ is not commutative, then Corollary 4.7 about the relationship between roots and factors is not true for $R$. The reason is that, when multiplying out $(x - \alpha) \cdot q(x)$ and collecting it back into the standard form of a polynomial, you have to move the $x$ from the left side to the right side of the coefficients of $q$ (let's call these coefficients $q_m, \ldots, q_1, q_0$). Since $R$ is not commutative, when you plug in $x = \alpha$, it might not be true that $\alpha q_i = q_i \alpha$. This means the equation

$$f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r$$

might be false.

For a ring like $R = \mathbb{Z}_6$, the problem is a subtler one. Using long division, you can check that each polynomial $x - [0]_6$, $x - [1]_6$, $x - [3]_6$, and $x - [4]_6$ is indeed a factor of $x^2 - x$, and that

$$x^2 - x = (x - [0]_6)(x - [1]_6) = (x - [3]_6)(x - [4]_6).$$

So the problem is that factorisations of polynomials in $R[x]$ might not be *unique*! There can be more than one factorisation with different factors.

In the proof of the Fundamental Theorem of Algebra with multiplicities in the notes, this point was completely glossed over. If a degree $n$ polynomial in $\mathbb{C}[x]$ had more than one factorisation into linear factors of the form $x - \alpha$, it would have more than $n$ roots as well, namely, $n$ roots (counting repeated roots) from the first factorisation and at least one more new root from the second. Don't worry, this isn't a problem with the Fundamental Theorem of Algebra itself. If $K$ is a field, like $\mathbb{C}$, it turns out that factorisations in $K[x]$ into factors $x - \alpha$ are always unique. To use the terminology that will be introduced in the module *Ring Theory* (where this will be proved), $K[x]$ is a *unique factorisation domain*.

Recall that, if $R$ is a ring, $\mathrm{M}_n(R)$ is our notation for the ring of $n \times n$ square matrices with elements of $R$ as entries.

**Question 4** If $x$ and $y$ are elements of a ring $R$ such that $xy = yx$, we say that $x$ and $y$ *commute*, or that $x$ *commutes with* $y$.

Find all matrices in $\mathrm{M}_2(\mathbb{R})$ which commute with $\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$.

**Solution** Take an arbitrary matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$ and multiply it on either side by the given matrix $\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix} = \begin{pmatrix} 3a-2b & 4a-3b \\ 3c-2d & 4c-3d \end{pmatrix}$$
$$\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 3a+4c & 3b+4d \\ -2a-3c & -2b-3d \end{pmatrix}$$

$A$ commutes with $\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$ if and only if these two products are equal, which happens if and only if corresponding entries are equal:

$$3a-2b = 3a+4c \qquad 4a-3b = 3b+4d$$
$$3c-2d = -2a-3c \qquad 4c-3d = -2b-3d$$

This is now a system of four linear equations in four real unknowns, which you can solve using any familiar method (isolate and substitute, Gaussian elimination, ...). You should get a set of solutions with two parameters: $a = -3c+d$, $b = -2c$, and $c$ and $d$ can be any real numbers. So the set of matrices that commute with $\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$ is

$$\left\{ \begin{pmatrix} -3c+d & -2c \\ c & d \end{pmatrix} : c,d \in \mathbb{R} \right\}.$$

*Commentary.* This is "typical" for which elements commute in a noncommutative ring. Any given element may still commute with many elements (in this case uncountably many); but still, if you pick two elements at random, it probably won't commute (in this case, $a = -3c+d$ and $b = -2c$ probably won't be true at random).

In fact, any element $A \in R$ must commute with all its powers $A^0 = 1_R$, $A$, $A^2$, $A^3$, ...: by the associative law,

$$A \cdot A^n = A \cdot (\underbrace{A \cdots A}_{n}) = \underbrace{A \cdots A}_{n+1} = (\underbrace{A \cdots A}_{n}) \cdot A = A^n \cdot A.$$

So $A$ also commutes with any sums and differences of these powers. In the matrix case, where $R = \mathrm{M}_n(K)$ for a field $K$, scalars also commute with matrices, so $A$ commutes with $f(A)$ for any $f \in K[x]$. If $A$ has $n$ distinct eigenvalues, then it turns out these are the only matrices which $A$ commutes with. The given matrix $\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$ does have two distinct eigenvalues, and its square is $I$, so any polynomial in $A$ with real scalar coefficients simplifies to $sI + tA$ for some $s,t \in \mathbb{R}$. Indeed, the answer given above is the same set as

$$\{sI + tA : s,t \in \mathbb{R}\} = \left\{ \begin{pmatrix} s+3t & 4t \\ -2t & s-3t \end{pmatrix} : s,t \in \mathbb{R} \right\}.$$

**Question 5** Let $R$ be a ring, and $n$ a natural number. Describe the rings $\mathrm{M}_n(R[x])$ and $\mathrm{M}_n(R)[x]$. Give an example of an element of each ring. Explain how these two rings relate to each other.

**Solution** $\mathrm{M}_n(R[x])$ is the ring of $n$-by-$n$ matrices whose entries are polynomials in the variable $x$ with coefficients in $R$, whereas $\mathrm{M}_n(R)[x]$ is the ring of polynomials in the variable $x$ whose coefficients are $n$-by-$n$ matrices with entries in $R$.

For example, when $n = 2$ and $R = \mathbb{Z}$, an element of each ring is given by

$$\begin{pmatrix} 1 & x-1 \\ -x & 1 \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}[x]),$$
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} x + \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})[x].$$

The relationship between these rings is, in informal language, that they are two different presentations of "the same ring". To start with, there is a bijection from one ring to the other. Given a polynomial of matrices, you can formally multiply the powers of $x$ through inside the matrices, sum the results, and end up with a matrix of polynomials. To go the other direction, given a matrix of polynomials over $R$, you can split it as a sum of matrices one of which contains only elements of $R$, one only elements of $R$ times $x$, one only elements of $R$ times $x^2$, etcetera, and then move the power-of-$x$ factors outside. The two examples above are related by this bijection.

But this is not enough to make the rings $\mathrm{M}_n(R[x])$ and $\mathrm{M}_n(R)[x]$ "the same" in an algebraist's eyes, since a ring is not just its set of elements; it also has rules for addition and multiplication. So the key facts are that, if you are adding or multiplying two matrices of polynomials, you'd get the same results if you instead translated to polynomials with matrix coefficients and worked the sum or product out in that language instead. Like many others in the past fortnight, the proofs of these facts don't need any tricks, but they can be difficult because of the book-keeping with notation and indices that you need to do.

I will show how this goes for addition, which is the less arduous of the two. A general element $F \in M_n(R[x])$ is a matrix $(f_{ij})_{n\times n}$ where $f_{ij} \in R[x]$ for each $1 \leq i, j \leq n$. By adding leading zeroes to each $f_{ij}$ to make them all have the same number of terms, we can write

$$f_{ij} = a_{ijm}x^m + \cdots + a_{ij1}x + a_{ij0}$$

for some collection of elements $a_{ijk} \in R$ ($1 \leq i, j \leq n$, $1 \leq k \leq m$). The corresponding element $F^* \in M_n(R)[x]$ is

$$F^* = A_m x^m + \cdots + A_1 x + A_0$$

where the matrix $A_k = (a_{ijk})_{n\times n}$ contains the entries $a_{ijk} \in R$, the same ones as above. Now let $G = (g_{ij})_{n\times n} \in M_n(R[x])$ and $G^* = B_m x^m + \cdots + B_0 \in M_n(R)[x]$ be a second pair of corresponding elements, built from the elements $b_{ijm} \in R$. Then

$$F + G = (f_{ij} + g_{ij})_{n\times n} = \big((a_{ijm} + b_{ijm})x^m + \cdots + (a_{ij0} + b_{ij0})\big)_{n\times n}$$

and

$$\begin{aligned} F^* + G^* &= (A_m + B_m)x^m + \cdots + (A_0 + B_0) \\ &= (a_{ijm} + b_{ijm})_{n\times n}x^m + \cdots + (a_{ij0} + b_{ij0})_{n\times n}. \end{aligned}$$

And we see that these two sums correspond in the same way that $F$ and $F^*$ correspond, and that $G$ and $G^*$ do: both are put together using the same collection of elements $a_{ijk} + b_{ijk} \in R$ ($1 \leq i, j \leq n$, $1 \leq k \leq m$).

If you take further modules in algebra, you will encounter the concept of *isomorphism*, a special kind of bijection between algebraic objects (like rings) that preserves their structure (for rings, this means addition and multiplication). This question gives an example of an isomorphism.