Queen Mary University of London

MTH4104 **Introduction to Algebra**

Extra questions for chapter 4 **Spring 2021**

These questions are for you to practice with on your own schedule. You may e.g. want to try some each week as their topics come up in lectures, or use them in exam revision.

4 Polynomials

4.1 Defining polynomials

Question 4.1.1 Let K be a skewfield, and let $f, g \in K[x]$ be two nonzero polynomials. Prove that $fg \neq 0$.

Solution Suppose that f has degree d and g has degree e. Since neither f nor g are zero, both of these degrees are well-defined. It follows that

$$f = a_d x^d + \cdots + a_1 x + a_0$$
$$g = b_e x^e + \cdots + b_1 x + b_0$$

where a_d and b_e are nonzero elements of R. Now, the product of f and g is the sum of a collection of terms like $a_i b_j x^{i+j}$. The only way the exponent $i+j$ of x in this term can be as large as $d+e$ is if $i = d$ and $j = e$, which are the largest possible values of i and j. Therefore

$$fg = a_d b_e x^{d+e} + (\text{terms with smaller powers of } x);$$

in other words, if we write

$$fg = c_n x^n + \cdots + c_1 x + c_0$$

in standard for, then $n = d+e$ and $c_n = a_d b_e$.

It is true in any skewfield that if $a_d \neq 0$ and $b_e \neq 0$ then $a_d b_e \neq 0$. This needs proof! A quick way to show it is that $a_d b_e$ has a multiplicative inverse, namely $b_e^{-1} a_d^{-1}$, while 0 cannot possibly have a multiplicative inverse. Having established this, it follows that the leading coefficient of fg is nonzero, and therefore fg is not the zero polynomial, as desired.

4.2 Polynomial rings

Question 4.2.1 Give a counterexample to the multiplicative inverse law for the ring $\mathbb{R}[x]$ of polynomials in x with real coefficients.

Use the properties of degree in question 2 from the week 8 tutorial sheet to prove that your counterexample is valid.

Solution One such counterexample is the polynomial $f = x$. That counterexample is, in fact, in the notes. What is interesting here is the alternative method of proof asked for.

We use proof by contradiction. Suppose that g was a multiplicative inverse of f, so that $fg = 1$ in $\mathbb{R}[x]$. Since degree is a well-defined function (except on the zero polynomial), we may take degree of both sides, and use the rule for multiplication:

$$1 + \deg(g) = \deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0.$$

This implies $\deg(g) = -1$, which is a contradiction: polynomials cannot have negative degree.

4.3 Roots and factors

Question 4.3.1 Let $f, g \in \mathbb{R}[x]$ be polynomials, with $\deg g > 0$. Suppose that $\deg f = 8$, and $(x-1)^3$ divides f. What can be said about the multiplicity of 1 as a root of f?

Solution If $f = (x-1)^m \cdot g$ where g is a polynomial that is not a multiple of $x-1$, then the multiplicity being asked for is m. We assume that $f = (x-1)^3 \cdot h$ for some polynomial h. Since h may have factors $x-1$ of its own, this implies that $m \geq 3$. On the other hand, $m \leq 8$, because $\deg(x-1)^m = m$, and if $m > 8$ then $\deg f$ would be greater than 8 as well by Question 3 from the week 8 coursework. Every integer m from 3 to 8 is attainable: consider $f = (x-1)^m x^{8-m}$.

Question 4.3.2 Let f and g be polynomials in $\mathbb{K}[x]$, where K is a field.

(a) Prove that if f divides g, then every root of f is also a root of g.

(b) Is the converse true? Justify your answer.

Solution (a) By definition, if f divides g, there is a polynomial $h \in K[x]$ such that $f \cdot h = g$. Then if α is an element of K such that $f(\alpha) = 0$, we have

$$g(\alpha) = f(\alpha) \cdot h(\alpha) = 0 \cdot h(\alpha) = 0$$

using the submission question on the week 8 coursework for the first equality, and Proposition 3.13 for the second.

(b) The converse is false. For example, let $K = \mathbb{R}$, $f = x^2$ and $g = x$. Then every root of f is a root of g, but f does not divide g. We can prove f does not divide g e.g.

using question 3 on the week 8 coursework, since the degree of f is greater than the degree of g. (Or we could work out the product with a polynomial with indeterminate coefficients and thereby prove it directly.)

Question 4.3.3 Let $\sim$ be the relation on the polynomial ring $\mathbb{R}[x]$ defined by

$$\sim = \{(p,q) \in \mathbb{R}[x]^2 : q - p = (x^2+1)\cdot r \text{ for some } r \in \mathbb{R}[x]\}.$$

(a) Prove that $\sim$ is an equivalence relation.

(b) Let K be the set of equivalence classes of $\sim$. Define addition and multiplication operations on K, and prove that they are well-defined.

(c) How is K related to $\mathbb{C}$?

Solution (a) This part and part (b) are just like the proofs for the equivalence relation $\equiv_m$.

For any $a \in \mathbb{R}[x]$, we have $a - a = (x^2+1)\cdot 0$, so $a \sim a$. This proves $\sim$ is reflexive.

Let a and b be polynomials in $\mathbb{R}[x]$ so that $a \sim b$, that is so that $b - a = (x^2+1)r$ for some $r \in \mathbb{R}[x]$. Then $a - b = (x^2+1)(-r)$, so $b \sim a$. This proves $\sim$ is symmetric.

Let a, b, and c be polynomials in $\mathbb{R}[x]$ such that $a \sim b$ and $b \sim c$. Then $b - a = (x^2+1)r$ and $c - b = (x^2+1)s$ for some polynomials $r, s \in \mathbb{R}[x]$. Adding these two equations,

$$c - a = (c-b) + (b-a) = (x^2+1)(r+s),$$

which shows that $a \sim c$. Therefore $\sim$ is transitive.

(b) Given two equivalence classes $[a]_\sim$ and $[b]_\sim$, we would like to define their sum and product as

$$\begin{aligned} [a]_\sim + [b]_\sim &= [a+b]_\sim \\ [a]_\sim [b]_\sim &= [ab]_\sim \quad . \end{aligned}$$

To show this is well defined, we need to show that if we had picked different representatives $c \in [a]_\sim$ and $d \in [b]_\sim$, then $[c+d]_\sim = [a+b]_\sim$ and $[cd]_\sim = [ab]_\sim$. Restated without congruence classes using our handy Corollary 3.7, what we have to show is that if $c \sim a$ and $d \sim b$, then $c + d \sim a + b$ and $cd \sim ab$.

Let $c - a = (x^2+1)r$ and $d - b = (x^2+1)s$ for real polynomials r and s. Solving, this means $c = a + (x^2+1)r$ and $d = b + (x^2+1)s$. Then

$$c + d = a + (x^2+1)r + b + (x^2+1)s = a + b + (x^2+1)(r+s)$$

so that $(c+d) - (a+b)$ is a multiple of x^2+1, proving $c + d \sim a + b$. Likewise,

$$cd = (a + (x^2+1)r)(b + (x^2+1)s) = ab + (x^2+1)(r + s + (x^2+1))$$

so that $cd - ab$ is a multiple of x^2+1, proving $cd \sim ab$. This is what was to be shown.

(c) The connection between K and $\mathbb{C}$ is best seen by changing the formal symbol from x to i. Then the equivalence classes of $\sim$ are classes of polynomial in i with real coefficients which differ by multiples of $\mathrm{i}^2 + 1$. But if i were the complex i, then $\mathrm{i}^2 + 1$ would

be 0 and the polynomials in a single equivalence class would all be equal anyway! It can also be shown that different equivalence classes give different complex numbers when $x = \mathrm{i}$: for example, use polynomial division by $x^2 + 1$ to show that each equivalence class contains a polynomial of degree at most 1.

In this way, K is actually "the same field as $\mathbb{C}$" in a different language. (Algebraists would say that K and $\mathbb{C}$ are *isomorphic*.)

Commentary. If we had used this question to give our original definition of $\mathbb{C}$, it would have saved us some effort in the proof that $\mathbb{C}$ is a field (at the cost of being a more obscure setup). To be precise, most of the field laws can be proved in K just by choosing representatives of the classes and then observing that the laws hold in $\mathbb{R}[x]$ which implies that they hold in K. The only law that we can't do this for is the multiplicative inverse law.

We used the same time-saving idea when we proved the structures $\mathbb{Z}_m$ were commutative rings with identity in Section 3.4 of the course notes.

Question 4.3.4 Let $f \in \mathbb{R}[x]$ be a polynomial and $\alpha \in \mathbb{R}$ a real number. Prove that α is a root of f of multiplicity at least 2 if and only if α is a root of both f and f', where f' is the derivative of f with respect to x.

The only Calculus facts you should need for this question are the sum and product rules: if $f, g \in \mathbb{R}[x]$, then

$$\begin{aligned}(f+g)' &= f' + g', \\ (fg)' &= f' \cdot g + f \cdot g'.\end{aligned}$$

Solution Suppose that α is a root of f of multiplicity at least 2. By the definition of multiplicity, this means that $(x-\alpha)^2$ divides f. Possibly even a larger power of $x-\alpha$ divides f, but if so $(x-\alpha)^2$ is a divisor too.

Therefore, we may write $f = (x-\alpha)^2 \cdot g$ for some polynomial $g \in \mathbb{R}[x]$. In particular,

$$f = (x-\alpha)\big((x-\alpha)\cdot g\big)$$

has $x-\alpha$ as a factor, so $f(\alpha) = 0$. Using the product rule,

$$\begin{aligned}f' &= 2(x-\alpha)\cdot g + (x-\alpha)^2 \cdot g' \\ &= (x-\alpha)\Big(2g + (x-\alpha)\cdot g'\Big)\end{aligned}$$

also has $x-\alpha$ as a factor, so $f'(\alpha) = 0$ as well.

Conversely, assume $f(\alpha) = f'(\alpha) = 0$. The former equation implies that $x-\alpha$ divides f, so we may write $f = (x-\alpha)\cdot h$ for some $h \in \mathbb{R}[x]$. Differentiating this equation using the product rule yields

$$f' = h + (x-\alpha)\cdot h'.$$

Substituting $x = \alpha$ now yields

$$\begin{aligned} 0 &= h(\alpha) + (\alpha - \alpha)h'(\alpha) \\ &= h(\alpha) + 0, \end{aligned}$$

using our second assumption. Therefore $h(\alpha) = 0$ and $h(\alpha)$ must itself have a factor of $x - \alpha$, implying that $f = (x - \alpha) \cdot h$ is in fact divisible by $(x - \alpha)^2$. As before, this is equivalent to α having multiplicity at least 2: whatever number is the actual largest power of $x - \alpha$ dividing f, i.e. the multiplicity, it must be at least 2.

4.4 Polynomial division

Question 4.4.1

(a) Let $f = t^{12} - 1$ and $g = t^5 - 1$. Using the Euclidean algorithm for polynomials, show that $\gcd(f, g) = t - 1$, and find polynomials x and y in $\mathbb{R}[t]$ such that $fx + gy = t - 1$.

(b) How is your answer to part (a) related to the Euclidean algorithm for integers?

Solution (a) The Euclidean algorithm for polynomials works just like that for integers. We start by dividing f by g using polynomial long division, obtaining a remainder b_2; then we divide g by b_2, obtaining a remainder b_3; and so on, until one of our remainders is zero.

So, first step, divide $t^{12} - 1$ by $t^5 - 1$. There are lots of zero coefficients in these polynomials, so to apply the polynomial long division algorithm, I should really write out the divisor as $t^5 + 0t^4 + 0t^3 + 0t^2 + 0t - 1$ and the quotient similarly, and I will have lots of steps where I subtract zero times the divisor. For a more concise presentation I will squeeze out all the columns with only zeroes from the below.

$$\begin{array}{rrrrrrrrrrrrr} & & & & & & t^7 & +t^2 & & & & & \\ \cline{7-13} t^5 & -1 & \big) & t^{12} & & & & & & & & & -1 \\ & & & t^{12} & & & -t^7 & & & & & & \\ \cline{4-7} & & & & & & t^7 & & & & & & \\ & & & & & & t^7 & & -t^2 & & & & \\ \cline{7-9} & & & & & & & & t^2 & & & & -1 \end{array}$$

The remainder is the first polynomial of degree less than 5 appearing, at which point we stop. Here it is $t^2 - 1$.

The next step is to divide $t^5 - 1$ by this remainder $t^2 - 1$. As before:

$$\begin{array}{rrrrrrrrrrrrr} & & & & & & t^3 & +t & & & & & \\ \cline{7-13} t^2 & -1 & \big) & t^5 & & & & & & & & & -1 \\ & & & t^5 & & & -t^3 & & & & & & \\ \cline{4-7} & & & & & & t^3 & & & & & & \\ & & & & & & t^3 & & -t & & & & \\ \cline{7-9} & & & & & & & & t & & & & -1 \end{array}$$

and the remainder is $t - 1$.

Next we divide t^2-1 by $t-1$. But, recognising the factorisation $t^2-1=(t+1)(t-1)$, we see that $t-1$ divides t^2-1 with remainder 0. So Euclid's algorithm stops at this point.

It remains to run the extended algorithm. Again we do the same as we do with integers, and substitute back for each of our remainders in turn:

$$\begin{aligned}
&t-1\\
&=(t^5-1)-(t^3+t)(t^2-1)\\
&=(t^5-1)-(t^3+t)\big((t^{12}-1)-(t^7+t^2)(t^5-1)\big)\\
&\quad=(-t^3-t)(t^{12}-1)+\big((t^3+t)(t^7+t^2)+1\big)(t^5-1)\\
&\quad=(-t^3-t)(t^{12}-1)+(t^{10}+t^8+t^5+t^3+1)(t^5-1).
\end{aligned}$$

So we conclude that $x=-t^3-t$ and $y=t^{10}+t^8+t^5+t^3+1$ is a solution.

(b) The general fact which I wanted you to observe in your computations from part (a) is: if a and b are integers such that $a \bmod b = r$, then the remainder when t^a-1 is divided by t^b-1 is t^r-1. To say (informally) why, each time we subtract a multiple of t^b-1 in the division algorithm, we reduce the polynomial we're working on from t^c-1 (for some $c\in\mathbb{Z}_{\geq 0}$ to $t^{c-b}-1$, except if $\deg t^c-1<\deg t^b-1$, that is $c<b$, in which case we're done. This corresponds precisely to computing a remainder by repeated integer subtraction.

Using this fact repeatedly shows that the Euclidean algorithm for these polynomials exactly tracks the Euclidean algorithm for integers, just with $t^{b_i}-1$ appearing instead of b_i. We conclude that $\gcd(t^a-1,t^b-1)=t^{\gcd(a,b)}-1$.

It is much trickier to interpret the more complicated polynomials x and y, and I wasn't expecting you to spot an interpretation. I will give a description without proof. Run the extended Euclidean algorithm for integers on a and b, producing integers X and Y such that $aX+bY=1$. Suppose without loss of generality that $X>0$ and $Y\leq 0$ (otherwise exchange a and b). Then

$$\begin{aligned}
x&=\sum_{i=0}^{X-1} t^{(ia) \bmod b},\\
y&=-\sum_{i=-Y}^{-1} t^{(ib) \bmod a}.
\end{aligned}$$

4.5 The Fundamental Theorem of Algebra

Question 4.5.1 Find all complex solutions z to the equation

$$z^8-2z^4+1=0$$

in standard form $z=a+b\mathrm{i}$, and state their multiplicities. Justify your answer.

Solution There is no general rule for solving general polynomial equations of degree 8, as pointed out in the supplementary notes, so we will have to use methods based on the special form of this polynomial. As the given polynomial is a quadratic in z^4, we can solve for z^4 as a first step. Since this is a real polynomial, you know how to solve it. The quickest way is to spot its factorisation:

$$(z^4-1)^2=0$$

implies that $z^4-1=0$. So we have reduced the problem to solving this single equation.

The solutions to $z^4-1=0$ are the *complex* fourth roots of 1. Don't jump to conclusions about what these are based on your knowledge of $\mathbb{R}$! One way to get these is by factoring further, recognising that

$$z^4-1=(z^2)^2-1^2=(z^2-1)(z^2+1).$$

So our solutions either satisfy $z^2-1=0$ or $z^2+1=0$. In the first case, z is a square root of 1, so $z=1$ or $z=-1$; the Fundamental Theorem of Algebra (with multiplicities) says that going to $\mathbb{C}$ gains you no more. In the second case, z is a square root of -1, so $z=\mathrm{i}$ or $z=-\mathrm{i}$.

When solving an equation, we must prove that all of our putative solutions $z=1,-1,\mathrm{i},-ii$ are in fact solutions, i.e. that we have not introduced any extraneous values. (Often when using standard techniques this is guaranteed – when they are used right! It is still good hygiene to check.) In this case, $z^4=1$ for all of our solutions, so the check amounts in every case to

$$z^8-2z^4+1=(1)^2-2\cdot 1+1=0.$$

The polynomial z^8-2z^4+1 has degree 8. Therefore, the version of the Fundamental Theorem of Algebra with multiplicities says that the sum of the multiplicities of the solutions equals 8. We have four solutions, and each of them has multiplicity at least 2, because of the factorisation $z^8-2z^4+1=(z^4-1)^2$ we found earlier: taking $z=1$ as example, $z-1$ divides z^4-1, so $(z-1)^2$ divides $(z^4-1)^2$. That means that each solution has multiplicity exactly 2 because the sum of the multiplicities we have accounted for already is 8; there is no room for more.

For another question on this topic, see the end of the extra document "Solving polynomial equations" on QMPlus.