Queen Mary University of London

MTH4104 Introduction to Algebra

Week 5 tutorial questions **w/c 21 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 Define the two sets

$$O = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, \gcd(a,b) = 1, b \text{ is odd} \right\}$$
$$E = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, \gcd(a,b) = 1, b \text{ is even}, b \neq 0 \right\}.$$

In other words, a fraction in simplest form belongs to O if its denominator is odd and to E if its denominator is even.

Is O a ring? Is O a field? Is E a ring? Is E a field? In the definitions of ring and field, use the ordinary addition and multiplication operations for rational numbers.

Solution E is not a ring. One of the ring axioms it does not satisfy is the additive closure law. A counterexample to the additive closure law is that $\frac{1}{2} \in E$, but $\frac{1}{2} + \frac{1}{2} = 1 \notin E$. Since E is not a ring and all fields are rings, E is not a field.

Bear in mind that you only have to name one violated axiom to justify that E is not a ring. There are more axioms it doesn't satisfy: another one is the additive identity law. The ultimate reason for this is that $0 \notin E$, but make sure you understand how saying that the rational number 0 is not in E is not by itself a counterexample to the additive identity law! You also need the observation that no other element of E could "play the role of" zero.

O is a ring. I will run quickly through the justification. Of the ring axioms, the associative, commutative and distributive laws are true for O because elements of O are just certain rational numbers, and these laws are true for all rational numbers. The additive identity law is true because $0 = 0/1 \in O$ is the additive identity element. For the additive closure law, let $a/b, c/d \in O$, written in simplest form. We know that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

The denominator bd is odd, so all of its factors are odd as well; therefore, after dividing out any common factors, the denominator of the sum is still odd. So $a/b + c/d \in O$.

The same kind of reasoning proves that $(a/b) \cdot (c/d) = ac/bd$ is in O, which is the multiplicative closure law. Finally, for the additive inverse law, the additive inverse of a/b is $(-a)/b$, which has the same denominator, so $a/b \in O$ implies $-a/b \in O$.

O is not a field. The single field axiom it does not satisfy is the multiplicative inverse law. A counterexample is that $2 = 2/1 \in O$ but 2 has no multiplicative inverse in O. Because we're using the usual multiplication of rational numbers the multiplicative inverse of 2 would still have to be $\frac{1}{2}$, but $\frac{1}{2} \notin O$.

Question 2

(a) What is the smallest subset of $\mathbb{R}$ that is a field?

(b) What is the smallest subset of $\mathbb{R}$ containing $\sqrt{2}$ that is a field?

(c) What is the smallest subset of $\mathbb{R}$ containing $\sqrt{2}$ and $\sqrt{3}$ that is a field?

Justify your answers. For all three parts, use the usual definitions of addition and multiplication for $\mathbb{R}$.

Solution If you thought of $\mathbb{Q}$ as an answer to (a), and couldn't think of any smaller set you've studied that is a field, then your thoughts are in the right place. But "I couldn't come up with anything smaller" isn't a good justification. We should base our reasoning on the field axioms.

The associative, commutative and distributive laws are true for any subset of $\mathbb{R}$, and if the subset contains 0 and 1 the nontrivial law is true as well. So the axioms which we have to pay attention to for this question are the identity, closure and inverse laws. If $K \subseteq \mathbb{R}$ is a field, the identity laws imply $0 \in K$ and $1 \in K$, because no other real numbers are possibilities for the identity elements. The closure laws state that K is closed under addition and multiplication. And the inverse laws state that K is closed under negation, and $K \setminus \{0\}$ is closed under reciprocals (again, the inverse of a real number in K cannot be different than its inverse in $\mathbb{R}$). Mathematical language reminder: "K is closed under negation", for example, means "given any element of K, its negative is also an element of K".

(a) If $K \subseteq \mathbb{R}$ is a field, the above closure properties force many real numbers to be elements of K. Since $1 \in K$, the additive closure law means $2 = 1 + 1 \in K$, then $3 = 2 + 1 \in K$, then $4 = 3 + 1 \in K \ldots$ indeed, all positive integers are in K. Because K is closed under negation and contains 0, in fact, all integers are elements of K. Because K is closed under reciprocals, all unit fractions $1/n$ are elements of K, where n is a nonzero integer. Finally, because K is closed under multiplication, all rational numbers are elements of K. In other words, $\mathbb{Q} \subseteq K$. But $\mathbb{Q}$ itself is a field! So $\boxed{\mathbb{Q}}$ is the answer to part (a).

(b) As above, any field $K \subseteq \mathbb{R}$ contains $\mathbb{Q}$. If K also contains $\sqrt{2}$, then by the additive and multiplicative closure laws, K contains every real number of the form $q + r\sqrt{2}$, where $q, r \in \mathbb{Q}$.

Do the axioms imply that any other numbers must be in K, or can we stop here? It turns out we can stop here: $\boxed{\{q + r\sqrt{2} : q, r \in \mathbb{Q}\}}$ is a field, so it is the answer to the

question. Mathematicians' usual notation[1] for this set $\{q+r\sqrt{2} : q,r \in \mathbb{Q}\}$ is $\mathbb{Q}(\sqrt{2})$. I'll use this notation for the rest of this answer.

To check that $\mathbb{Q}(\sqrt{2})$ is a field, since it contains 0 and 1, we only need to check the closure laws. Let $q+r\sqrt{2}$ and $s+t\sqrt{2}$ be elements of $\mathbb{Q}(\sqrt{2})$, where $q,r,s,t \in \mathbb{Q}$.

Additive closure $(q+r\sqrt{2})+(s+t\sqrt{2}) = (q+s)+(r+t)\sqrt{2}$ is in $\mathbb{Q}(\sqrt{2})$ because $q+s$ and $r+t$ are rational numbers.

Additive inverse $-(q+r\sqrt{2}) = (-q)+(-r)\sqrt{2}$ is in $\mathbb{Q}(\sqrt{2})$ because $-q$ and $-r$ are rational numbers.

Multiplicative closure $(q+r\sqrt{2})(s+t\sqrt{2}) = (qs+2rt)+(qt+rs)\sqrt{2}$ is in $\mathbb{Q}(\sqrt{2})$ because $qs+2rt$ and $qt+rs$ are rational numbers. For this axiom, it was important that $(\sqrt{2})^2 = 2$ so that we could collect the rt term into the rational part of the product.

Multiplicative inverse By rationalising the denominator, as long as q and r are not both 0,

$$\frac{1}{q+r\sqrt{2}} = \frac{q-r\sqrt{2}}{q^2-2r^2} = \frac{q}{q^2-2r^2} + \frac{-r}{q^2-2r^2}\sqrt{2}.$$

Because $\sqrt{2}$ is irrational, the denominator q^2-2r^2 is nonzero, and so $q/(q^2-2r^2)$ and $-r/(q^2-2r^2)$ are rational numbers, proving this inverse is in $\mathbb{Q}(\sqrt{2})$.

(c) This part is similar to part (b). The main thing you need to notice is that, since $\sqrt{2}\cdot\sqrt{3} = \sqrt{6}$, the set $\{q+r\sqrt{2}+s\sqrt{3} : q,r,s \in \mathbb{Q}\}$ is not closed under multiplication. But

$$\boxed{\{q+r\sqrt{2}+s\sqrt{3}+t\sqrt{6} : q,r,s,t \in \mathbb{Q}\}}$$

is, and this is the field we seek. Mathematicians usually denote this $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

The arguments for additive closure and inverse and multiplicative closure are just like part (b), so I won't write them out again. For the multiplicative inverse law, how do you handle $1/(q+r\sqrt{2}+s\sqrt{3}+t\sqrt{6})$? One way is to first "$\mathbb{Q}(\sqrt{2})$-ise" the denominator and then fully rationalise it:

$$\frac{1}{(q+r\sqrt{2})+(s+t\sqrt{2})\sqrt{3}} = \frac{(q+r\sqrt{2})-(s+t\sqrt{2})\sqrt{3}}{(q+r\sqrt{2})^2-3(s+t\sqrt{2})^2}$$

and you can finish rationalising it yourself from there.

If you're really paranoid you might have asked questions like this: how do we know that $\sqrt{6}$ is not already an element of $\{q+r\sqrt{2}+s\sqrt{3} : q,r,s \in \mathbb{Q}\}$? Here's a very sketchy outline of a proof by contradiction, for you to fill in the details. Assume $\sqrt{6}$ was in that set. Clear denominators to get $a,b,c,d \in \mathbb{Z}$, $d \neq 0$, with $a+b\sqrt{2} = c\sqrt{3}+d\sqrt{6}$. Square both sides. Since $\sqrt{2}$ is irrational you can equate the real parts and the coefficients of $\sqrt{2}$. Isolate the square of a variable from the first equation; substitute into the square of the second; factor; get a contradiction because $\sqrt{3}$ and $\sqrt{6}$ are irrational.

[1] $\mathbb{Q}(\sqrt{2})$ is pronounced "Q adjoin root 2". To be clear, you were not expected to know this notation!

Question 3 Write down a complete proof of the right distributive law for multiplication in $\mathbb{C}$.

[That is, don't only write down the manipulation of equations in the middle; you should have some opening and closing text.]

Solution We must prove that for all $u, v, w \in \mathbb{C}$, the equation

$$(u+v)w = uw + vw$$

holds. Write the given complex numbers $u = a + b\mathrm{i}$, $v = c + d\mathrm{i}$, $w = e + f\mathrm{i}$ where a through f are real. Then

$$\begin{aligned}(u+v)w &= ((a+b\mathrm{i}) + (c+d\mathrm{i}))(e+f\mathrm{i}) = ((a+c) + (b+d)\mathrm{i})(e+f\mathrm{i}) \\ &= (a+c)e - (b+d)f + ((a+c)f + (b+d)e)\mathrm{i} \\ &= (ae + ce - bf - df) + (af + cf + be + de)\mathrm{i}\end{aligned}$$

whereas

$$\begin{aligned}uw + vw &= (a+b\mathrm{i})(e+f\mathrm{i}) + (c+d\mathrm{i})(e+f\mathrm{i}) \\ &= ((ae-bf) + (af+be)\mathrm{i}) + (ce-df) + (cf+de)\mathrm{i}) \\ &= (ae - bf + ce - df) + (af + be + cf + de)\mathrm{i}.\end{aligned}$$

The two expressions are equal (since $a, \ldots, f$ are just real numbers and we take their properties for granted). This completes the proof.

Question 4 Let R be the set of all functions from $\mathbb{Z}$ to $\mathbb{Z}$, with addition defined by addition of values,

$$(f+g)(x) = f(x) + g(x) \qquad \text{for all } x \in \mathbb{Z},$$

and multiplication defined as composition,

$$(f \cdot g)(x) = f(g(x)) \qquad \text{for all } x \in \mathbb{Z}.$$

Prove that R is *not* a ring when given these operations. In other words, find a ring axiom that is not satisfied, and give a counterexample.

Solution This structure R is not a ring because it fails to satisfy the right distributive law. That is, it is not always true that

$$fg + fh = f(g+h)$$

for $f, g, h \in R$.

Here is a counterexample. Let g and h both be the identity function, while f is the function $f(x) = x^2$. Then we can compare the values of $fg + fh$ and $f(g+h)$ at any integer x:

$$(fg+fh)(x) = (fg)(x) + (fh)(x) = f(g(x)) + f(h(x)) = x^2 + x^2 = 2x^2$$

but

$$(f(g+h))(x) = f((g+h)(x)) = f(g(x) + h(x)) = f(2x) = 4x^2.$$

So we see that they are unequal functions.

As it turns out, R satisfies all the other axioms of rings with identity, including the left distributive law.