MTH4104 **Introduction to Algebra**

Extra questions for chapter 3 **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.

3 Algebraic structures

3.1 Rings and fields

I have combined this section and the following into a single list of questions in this document.

3.2 Understanding the axioms

Question 3.2.1 Let $m \geq 2$ be an integer.

(a) Prove that the set $m\mathbb{Z} := \{mk : k \in \mathbb{Z}\}$ is a ring, with the usual definitions of addition and multiplication on the integers.

[This question does not take as much work as it seems, because $m\mathbb{Z}$ is a subset of $\mathbb{Z}$. This means that some of the ring axioms for $m\mathbb{Z}$ follow immediately from the corresponding axiom for $\mathbb{Z}$. Look out for these.]

(b) Prove that $m\mathbb{Z}$ is not a ring with identity.

["$1 \notin m\mathbb{Z}$" is *not* a proof by itself! Remember that the "1" in the law can stand for any element of the ring.]

Question 3.2.2 Let X be a non-empty set and let $S = \mathscr{P}(X)$ be the set of all its subsets. Define operations of addition and multiplication on S by the rules

$$A + B := (A \cup B) \setminus (A \cap B)$$

and

$$AB := A \cap B$$

for any $A, B \in S$.

(a) Prove that S is a ring.

[I will accept Venn diagram "proofs", but if you do this, please still use full sentences to explain your argument. In your proofs, you should be exceedingly clear which elements you have selected as the identity elements ("0" and "1").]

(b) Is S a ring with identity? a skewfield? a commutative ring?

Question 3.2.3 Give an example of a ring that is neither commutative nor a ring with identity. Justify your answer. You need not give a complete proof, but you should give

(a) a counterexample to the commutative law for multiplication;

(b) an proof that your ring contains no multiplicative identity element;

(c) a general reason for why the ring axioms are true. This can be short but, as always, should be in complete sentences.

[Hint: try to "build" your example from rings you have seen with useful properties in the notes or other module material. If you have not yet seen an example of a non-commutative ring, come back to this question after you have.]

3.3 The complex numbers

Question 3.3.1 Find the real and imaginary parts of $\dfrac{-3+5\mathrm{i}}{2-9\mathrm{i}}$.

Question 3.3.2 Solve the linear equation

$$3(1-\mathrm{i})z-2=2z+\mathrm{i}+1.$$

Include a check that your answer is correct.

Question 3.3.3 Write up careful proofs of all of the field axioms for $\mathbb{C}$.

Question 3.3.4 If $z=a+b\mathrm{i}$ is a complex number, then its *conjugate* is defined to be $\overline{z}=a-b\mathrm{i}$.

(a) Prove that, if z and w are complex numbers, then $\overline{z}+\overline{w}=\overline{z+w}$ and $\overline{z}\cdot\overline{w}=\overline{zw}$.

(b) Prove that also $\overline{z}-\overline{w}=\overline{z-w}$ and, if w is nonzero, $\overline{z}/\overline{w}=\overline{z/w}$.

If you've done part (a), you could do this part similarly, by imitating that proof. Can you see, instead, how to *use* part (a) to prove this with less tedium?

(c) If you take any arithmetic expression in complex numbers, and transform it by replacing every number in it by its conjugate, the transformed expression evaluates to the conjugate of the value of the original expression. Write up a clear explanation of why this is true, in view of parts (a) and (b).

Question 3.3.5 Define addition and multiplication operations on the set $U=\mathbb{R}^2$ by

$$(a,b)+(c,d)=(a+c,\,b+d),$$
$$(a,b)\cdot(c,d)=(ac,\,ad+bc).$$

(a) Name the multiplicative identity element in U, and prove the multiplicative identity law.

(b) Prove that, if $a\neq 0$, then (a,b) has a multiplicative inverse in U.

Question 3.3.6 Let U be the set of expressions of the form $a + bu$ where a and b are real numbers. The u is a formal symbol. We want to make U into a ring similar to how we defined $\mathbb{C}$ as a ring, and we'd like u to satisfy the equation $u^2 = 2u - 2$.

(a) Provide the formulas we should use to define $+$ and $\cdot$ in U.

(b) Using your definitions, prove in U:

   (i) the identity laws for addition and multiplication;

   (ii) the associative law for multiplication.

(c) Is the inverse law for multiplication true in U?

3.4 Rings from modular arithmetic

Question 3.4.1 Write up a complete proof that $\mathbb{Z}_m$ is a commutative ring with identity, where $m > 0$ is an integer.

Question 3.4.2 Let F be the set $\{a + bI : a, b \in \mathbb{Z}_3\}$, where I is a formal symbol. Define operations of addition and multiplication on F by

$$(a + bI) + (c + dI) = (a + c) + (b + d)I,$$
$$(a + bI) \cdot (c + dI) = (ac - bd) + (ad + bc)I.$$

These definitions are meant to make I behave like a square root of $[-1]_3$.

(a) How many elements does F have?

(b) Prove the left distributive law in F.

(c) Name the additive identity element in F, and prove the additive identity law.

(d) Prove the multiplicative inverse law in F.

Like Question 1, F is in fact a field, and you could prove the other axioms if you wanted more practice. Of all the field axioms, the multiplicative inverse law (part (d)) is the one most different from the complex numbers.

(e) Can you interpret F as a set of congruence classes for a relation in some ring, the way $\mathbb{Z}_3$ is a set of congruence classes for a relation on $\mathbb{Z}$, with addition and multiplication defined in the analogous way?

For more questions on $\mathbb{Z}_m$, see the extra questions for Chapter 2.

For another question on a ring constructed in the same way as $\mathbb{Z}_m$ was, by defining operations $+$ and $\cdot$ on a set of congruence classes, see the extra questions on Chapter 4 (once I've posted them!) for a question about an equivalence relation on the ring $\mathbb{R}[x]$ of polynomials with real coefficients.

3.5 Properties of rings

Question 3.5.1 Let R be a ring with identity which does *not* satisfy the nontriviality axiom. Prove that R has only one element.

Question 3.5.2

(a) Fill in the blank in the following assertion with the name of a kind of ring.

> Let R be a ________. Then the identity $x^2 - y^2 = (x+y) \cdot (x-y)$ is true for all x and y in R.

The kind of ring you name should have as few axioms as possible.

(b) Prove the assertion from part (a). Name the ring axiom or fact that you are using at each step of your proof.

When you're done, check which axioms you've used. Could you have named a more general kind of ring in part (a)?

Question 3.5.3 Let R be a ring with identity and a be an element of R such that $a^n = 0$ for some positive integer n. Prove that $1 - a$ has a multiplicative inverse in R.