MTH6158 Ring Theory: Guide to Coursework 1

Note: This guide is meant to help you understand and carry out the problem solutions on your own. It is **not** meant to provide complete solutions!

1. *For each of the following algebraic structures, determine which of the axioms of a field they satisfy. Briefly explain your answers.*

   (a) *The set* $\mathbb{R}$ *of real numbers, with addition* $a \oplus b := \min(a, b)$ *and multiplication* $a \odot b := a + b$.

   This structure satisfies all the axioms of a field except for the zero law (A2) and the negation law (A3) (this last one does not even make sense, because there is no zero).

   In this structure, the (multiplicative) identity is the number 0. The multiplicative inverse of any number a is the number $-a$.

   Make sure you understand why all these statements are true!

   (b) *The collection* $\mathcal{P}(\mathbb{Z})$ *of subsets of* $\mathbb{Z}$, *with addition* $A \oplus B := A \Delta B$ *(symmetric difference) and multiplication* $A \odot B := A \cap B$.

   This structure satisfies all the axioms of a commutative ring with identity, but it is not a field (it does not satisfy axiom (M3) about the existence of multiplicative inverses).

   Axioms like associativity of addition (A1) or distributivity (D) can be argued by showing an equality between two Venn diagrams. The zero element is the empty set $\emptyset$. The additive inverse of any element A is A itself. The (multiplicative) identity is the whole set $\mathbb{Z}$.

2. *Suppose* R *is a ring in which* $a^2 = a$ *for all* $a \in R$. *(Such a ring is called a* Boolean ring.*) By considering elements of the form* $(x + y)^2$, *show that*

   (a) $a + a = 0$ *for all* $a \in R$.

   Suppose $a \in R$. Since the square of any element is equal to itself, we have $(a + a)^2 = a + a$. Expand this equation out carefully, using distributivity, and then use the cancellation law.

   (b) R *is a commutative ring.*

   Suppose $a, b \in R$. As the square of any element is equal to itself, we have $(a + b)^2 = a + b$. Again, expand this out and use the cancellation law to conclude that $a \cdot b = b \cdot a$.

3. *For each of the following rings R and subsets $S \subseteq R$, either prove that S is a subring of R or provide a counterexample to show that S is not a subring of R.*

   (a) $R = \mathbb{R}$, *and* $S = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$.

   The subset S is a subring of R. To prove this, let's use the subring test:

   (S0) The subset S is nonempty, because, for example, it contains the real number $0 = 0 + 0\sqrt{3}$.

   Now, let's take any two elements $s_1, s_2 \in S$. By definition, they must have the form $s_1 = a_1 + b_1\sqrt{3}$ and $s_2 = a_2 + b_2\sqrt{3}$, with $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

   (S1) Their difference is

$$s_1 - s_2 = (a_1 + b_1\sqrt{3}) - (a_2 + b_2\sqrt{3}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{3}.$$

   Since both $a_1 - a_2$ and $b_1 - b_2$ are integers, this last expression for $s_1 - s_2$ shows that it is an element of S.

   (S2) Their product is

$$s_1 s_2 = (a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}) = (a_1 a_2 + 3b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{3}.$$

   Both $a_1 a_2 + 3b_1 b_2$ and $a_1 b_2 + a_2 b_1$ are integers, so this expression for $s_1 s_2$ shows that it is an element of S.

   By the subring test, we therefore conclude that S is a subring of R.

   (b) $R = \mathrm{M}_{2\times 2}(\mathbb{R})$, *and* $S = \{A \in R : A \text{ is symmetric}\}$.

   The subset S is not a subring of R, as it is not closed under multiplication. You should be able to construct a concrete counterexample with two symmetric matrices whose product is not symmetric.

4. *Consider the ring $R = \mathcal{P}(\{a, b, c, d\})$, with addition equal to symmetric difference and multiplication equal to intersection, and its subring $S = \mathcal{P}(\{a, b\}) \subseteq R$.*

   (a) *Are R and S rings with identity? If so, write down their identity elements explicitly.*

   Both R and S are rings with identity. The identity element of R is the whole set $\{a, b, c, d\}$. However, this is not the identity of S! Instead, the identity of S is the set $\{a, b\}$. This is an example where a subring S has a different multiplicative identity than the ring R where it lives. In the lectures we showed that this phenomenon cannot happen for the additive identity — make sure you understand why the proof we gave there does not apply in the multiplicative case.

   (b) *How many cosets of S in R are there? List them all explicitly.*

Since R has 16 elements and S has 4 elements, there are $\frac{16}{4} = 4$ cosets of S in R. Explicitly, the 4 cosets are:

$$\{\, \emptyset \,,\, \{a\} \,,\, \{b\} \,,\, \{a,b\} \,\}$$
$$\{\, \{c\} \,,\, \{a,c\} \,,\, \{b,c\} \,,\, \{a,b,c\} \,\}$$
$$\{\, \{d\} \,,\, \{a,d\} \,,\, \{b,d\} \,,\, \{a,b,d\} \,\}$$
$$\{\, \{c,d\} \,,\, \{a,c,d\} \,,\, \{b,c,d\} \,,\, \{a,b,c,d\} \,\}$$

Make sure you understand well why this is the case!

5. *Consider the ring $R = \mathcal{P}(\{a,b\})$, with addition equal to symmetric difference and multiplication equal to intersection. Let $\mathrm{M}_{2\times 2}(R)$ be the ring of 2×2 matrices with entries in R.*

   (a) *How many elements does R have? How many elements does $\mathrm{M}_{2\times 2}(R)$ have?*

   The ring R has 4 elements. There are thus 4 possibilities for every entry of a matrix in $\mathrm{M}_{2\times 2}(R)$, which means there are a total of $4^4 = 256$ elements in $\mathrm{M}_{2\times 2}(R)$.

   (b) *Is $\mathrm{M}_{2\times 2}(R)$ a ring with identity? If so, write down the identity element explicitly.*

   Just like matrices with real entries, the ring $\mathrm{M}_{2\times 2}(R)$ is a ring with identity. Taking into account that the zero element of R is $\emptyset$, and the identity of R is $\{a,b\}$, one can check that the identity of $\mathrm{M}_{2\times 2}(R)$ is equal to

$$I = \begin{pmatrix} \{a,b\} & \emptyset \\ \emptyset & \{a,b\} \end{pmatrix}.$$

   (c) *Is $\mathrm{M}_{2\times 2}(R)$ a commutative ring? Justify your answer.*

   Just like matrices with real entries, the ring $\mathrm{M}_{2\times 2}(R)$ is not commutative. For example

$$\begin{pmatrix} \emptyset & \{a,b\} \\ \emptyset & \emptyset \end{pmatrix} \cdot \begin{pmatrix} \emptyset & \emptyset \\ \{a,b\} & \emptyset \end{pmatrix} = \begin{pmatrix} \{a,b\} & \emptyset \\ \emptyset & \emptyset \end{pmatrix},$$

   but

$$\begin{pmatrix} \emptyset & \emptyset \\ \{a,b\} & \emptyset \end{pmatrix} \cdot \begin{pmatrix} \emptyset & \{a,b\} \\ \emptyset & \emptyset \end{pmatrix} = \begin{pmatrix} \emptyset & \emptyset \\ \emptyset & \{a,b\} \end{pmatrix}.$$

   (d) *Is $\mathrm{M}_{2\times 2}(R)$ a division ring? Justify your answer.*

   Just like matrices with real entries, the ring $\mathrm{M}_{2\times 2}(R)$ is not a division ring, as not every matrix is invertible. For instance, check that the element $\begin{pmatrix} \emptyset & \emptyset \\ \emptyset & \{a,b\} \end{pmatrix}$ has no (right) multiplicative inverse, meaning that the following equation has no solution:

$$\begin{pmatrix} \emptyset & \emptyset \\ \emptyset & \{a,b\} \end{pmatrix} \cdot \begin{pmatrix} ? & ? \\ ? & ? \end{pmatrix} = \begin{pmatrix} \{a,b\} & \emptyset \\ \emptyset & \{a,b\} \end{pmatrix}.$$

6. *Consider the ring* $R = \mathrm{M}_{2\times 2}(\mathbb{R})$*, and its subset*

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subseteq R.$$

(a) *Show that* S *is a subring of* R*.*

You can use the subring test. First, show that S is nonempty by giving an example of a matrix in S. Then, take two arbitrary matrices in S, compute their difference, and check that it is a matrix in S. Lastly, take two matrices in S, compute their product, and check that it is a matrix in S.

(b) *Prove that* S *is isomorphic to the field* $\mathbb{C}$ *of complex numbers.*

We must show that S is basically the same ring as $\mathbb{C}$, but with different names for its elements. This can be done by giving an explicit relabelling, or isomorphism. Take $\theta : S \to \mathbb{C}$ defined as

$$\theta\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi.$$

You should prove that θ is injective, surjective, and a homomorphism. None of this is too difficult! This isomorphism provides what is often called the "matrix representation" of complex numbers.