Chapter 1

What is a Ring?

1.1 Lecture 1: Some Examples

Here are some sets of mathematical objects in which we can add, subtract and "multiply" elements together (without leaving the set). All of these are examples of *rings*. A ring is an algebraic structure equipped with two binary operations (generally called addition and multiplication) with some rules about how those operations behave and how they interact. Details of those rules are coming in Lecture 2.

1. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ - the set of *integers*.
2. $\mathbb{Q} = \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\right\}$ - the set of *rational numbers*.
3. $M_2(\mathbb{R})$ - the set of 2×2 matrices whose entries are real numbers.
4. $\mathbb{Q}[X] = \{a_k X^k + a_{k-1} X^{k-1} + \dots a_1 X + a_0 : a_i \in \mathbb{Q}, k \in \mathbb{Z}, k \geqslant 0\}$ - the set of *polynomials* in X with coefficients in $\mathbb{Q}$.
5. $C(\mathbb{R})$ - the set of *continuous* functions from $\mathbb{R}$ to $\mathbb{R}$ (where $\mathbb{R}$ is the set of *real numbers*). Addition is defined by
$$(\underbrace{f+g}_{\text{addition in } C(\mathbb{R})})(x) = \underbrace{f(x) + g(x)}_{\text{addition in } \mathbb{R}},$$
for $x \in \mathbb{R}$ and a pair of functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$.
The multplication in this example is function composition, defined by
$$(\underbrace{f \circ g}_{\text{multiplication in } C(\mathbb{R})})(x) = \underbrace{f(x) \times g(x)}_{\text{multiplicaton in } \mathbb{R}},$$
for $x \in \mathbb{R}$ and functions $f, g \in C(\mathbb{R})$.
6. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ - the set of congruence classes of integers modulo 6. Multiplication and addition here are modulo 6.
7. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ - the *complex numbers* (where $i^2 = -1$).
8. Let S be any set (for example $S = \{a, b, c, d, e\}$). Let $\mathcal{P}(S)$ be the *power set* of S - the set of all subsets of S (if S has n elements, then $\mathcal{P}(S)$ has 2^n elements). We can define "addtion" and "multiplication" on $\mathcal{P}(S)$ as follows, for subsets A and B of S.
   - we define the "sum" of A and B to be the *symmetric difference* of A and B. This is denoted $A \triangle B$ and consists of those elements that belong either to A or to B but not both. For example
   $$\{a, b, d, e\} \triangle \{c, b, d\} = \{a, c, e\}.$$

- We define the "product" of A and B to be the intersection $A \cap B$. For example

$$\{a, b, d, e\} \cap \{c, b, d\} = \{b, d\}.$$

The rest of this lecture consists of some observations about these examples and properties of their operations.

What do all the eight sets described above have in common as algebraic structures[1]? What disinguishes them?

Each of them is equipped with two binary operations called addition and multiplication. This is a similarity, even though the elements of the different sets don't necessarily resemble each other. Now we'll look at how these operations behave in each case, and identify some resemblances and some differences.

The Closure Property

All of the sets are *closed* under both the addition and multiplication operations. This means that within any of our sets, if we choose a pair of (not necessarily different elements) and add or multiply them, the result is still in the set. This property is part of the meaning of the statement that addition and multiplication are *binary operations* on the sets, but it is also worth noting explicitly because it arises a lot. An example of a set that is *not* closed under addition is the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ of the first 10 positive integers: we can add two elements of this set together, but their sum might not be in the set, for example $5 + 7$ is not.

Identity Elements for Addition

In each of our examples, the set contains an *identity element* or *neutral element* for addition. This has no effect when added to another element, like the number zero in any familiar number system: adding zero to another number has no effect, it is the same as doing nothing. For this reason, the identity element for addition in a ring is called the *zero element*, even if it is not actually the number zero, it behaves in a similar way.

Exercise In each of our examples, what is the zero element? Check below for the answers. Think about what you would need to write to explain any of these (one example of this is below).

1. The integer 0.
2. The rational number 0.
3. The zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
4. The function $f_0 : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 0, \ \forall\, x \in \mathbb{R}$.
   To see this, let f be any element of $C(\mathbb{R})$. For any $x \in \mathbb{R}$,

   $$(f + f_0)(x) = f(x) + f_0(x) = f(x) + 0 = f(x).$$

   So $f + f_0 = f$ (and also $f_0 + f = f$). This is saying that adding f_0 to f does not change f. This is true for every $f \in C(\mathbb{R})$, which means that f_0 is an identity element for addition in $C(\mathbb{R})$.
5. The zero polynomial 0.
6. The congruence class $\bar{0}$ modulo 6.
7. The complex number 0 $(= 0 + 0i)$.
8. The empty set (think about this one!).

Identity Elements for Multiplication

Each of these examples contains an identity element for multiplication, i.e. an element e for which $e \times a = a \times e = a$ for all elements a of the set; multiplying by e has no effect. The multiplicative identities are

[1] An algebraic structure is a non-empty set that is equipped with at least one binary operation, i.e. a means of combining any pair of elements of the set to produce an element of the set, like addition, subtraction, multiplication etc

1. The integer 1
2. The rational number 1
3. The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
4. The function $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 1$ for all $x \in \mathbb{R}$
(Exercise: explain this one - remember that multiplication means function composition here).
5. The polynomial 1
6. The congruence class $\bar{1}$ modulo 6
7. The complex number 1 $(= 1 + 0i)$
8. The full set S. (Why?)

The addition operation in our examples

- In all of our examples, addition is *commutative*, i.e. $a + b = b + a$ for all pairs a and b of elements. Check this.
- The addition operation is *associative* in all the examples. This means that $(a + b) + c = a + (b + c)$ for all elements a, b, c. In most cases this follows from the fact that addition of integers and real numbers is associative. In the last example, it is not completely obvious that the symmetric difference is an associative operation. To show this is an exercise. You could start by showing that for three sets A, B, C, the set $(A \triangle B) \triangle C$ consists of all of those elements that belong either to exactly one of A, B, C or to the intersection of all three of them.
- In each of our sets, every element has an additive inverse or "negative". Two elements are additive inverses each other if their sum is the zero element. The fact that every element of a set has an additive inverse means that subtraction can be defined in the set. Again, the last example is probably the one where this is not so easy to see. Given a set S, what set T has the property that $S \triangle T$ is the empty set?

The multiplication in our examples

- The multiplication operation is associative in all the examples.
- The multiplication is commutative in all of the examples except for $M_2(\mathbb{R})$ and $C(\mathbb{R})$. Neither matrix multiplication nor function composition are commutative. For 2×2 matrices A and B, the products AB and BA need not be equal. For a pair of functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$, the compositions $f \circ g$ and $g \circ f$ are generally not the same.
- Two elements are multiplicative inverses of each other if their product is the multiplicative identity element. In $\mathbb{Q}$, every element except 0 has a multiplicative inverse, namely its reciprocal. In $\mathbb{C}$, every non-zero element has an inverse for multiplication. For a non-zero complex number $z = a + bi$, its multiplicative inverse is $\frac{1}{a^2+b^2}(a - bi)$. All the other examples contain non-zero elements without multiplicative inverses (confirm this!).

The eight algebraic structures mentioned in this section are all examples of *rings*.