Chapter 1

What is a Ring?

1.1 Some Examples

Consider the following sets :

1. $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$ – the set of *integers*.
2. $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$ – the set of *rational numbers*.
3. $M_2(\mathbb{R})$ – the set of 2×2 matrices with real numbers as entries.
4. $2\mathbb{Z} = \{\dots, -2, 0, 2, 4, \dots\}$ – the set of *even integers*.
5. $C(\mathbb{R})$ – the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.
6. $\mathbb{Q}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \mid a_n, \dots, a_0 \in \mathbb{Q}\}$ – the set of polynomials with rational coefficients.
7. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ – the set of congruence classes in $\mathbb{Z}$ modulo 6.

Remember the very general definition of an *algebraic structure* as a set equipped with a *binary operation*, that is a scheme for combining any pair of elements of the set to produce a new element *of the same set*. All of the sets in our list above have binary operations defined on them in natural and probably mostly familiar ways. Of course it is possible for a set to have more than one "natural" binary operation defined on it. Algebra, in its broadest sense, is the study of algebraic structures.

What do all the six sets described above have in common as algebraic structures?

Each of them is equipped with two binary operations called addition and multiplication. In $\mathbb{Z}$, $\mathbb{Q}$ and $2\mathbb{Z}$ we have the usual addition and multiplication of integers and rational numbers. In $M_2(\mathbb{R})$ we have matrix addition and matrix multiplication. In $C(\mathbb{R})$ we have addition and multiplication defined by

$$(\underbrace{f+g}_{+\ in\ C(\mathbb{R})})(x) = \underbrace{f(x)+g(x)}_{+in\mathbb{R}},\ \text{for all } x \in \mathbb{R} \text{ and all } f, g \in C(\mathbb{R})$$

$$(\underbrace{f \times g}_{\times \text{ in } C(\mathbb{R})})(x) = \underbrace{f(x) \times g(x)}_{\times \text{in} \mathbb{R}}, \text{ for all } x \in \mathbb{R} \text{ and all } f, g \in C(\mathbb{R}).$$

In $\mathbb{Q}[x]$ we have the usual addition and multiplication of polynomials, e.g.

$$(x^2 + 2x + 4) + (x^3 - 3x + 2) = x^3 + x^2 - x + 6,$$

$$(x^2 - 2x + 1)(x + 5) = x^3 + 5x^2 - 2x^2 - 10x + x + 5 = x^3 + 3x^2 - 9x + 5.$$

In $\mathbb{Z}/6\mathbb{Z}$ the addition and multiplication are defined modulo 6, e.g. $\bar{4} + \bar{5} = \bar{3}$; $\bar{4} \times \bar{5} = \bar{2}$, etc.

Note: In each case the set under consideration is *closed* under the relevant operations of addition and multiplication; this means that in each case the product and sum of a pair of elements in a particular set also belong to that set. For example the set of odd integers is *not* closed under addition, since the sum of two odd integers is not odd.

Addition in our Examples

- All the above examples contain an identity element for addition, which we refer to as the zero element and write as 0. This element has the property that adding it to another element has no effect. The zero elements in our examples are

  1. The integer 0
  2. The rational number 0
  3. The zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
  4. The integer 0
  5. The function $f_0 : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 0$, $\forall\, x \in \mathbb{R}$
  6. The zero polynomial 0
  7. The congruence class $\bar{0}$ modulo 6

- 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.

- In all of our sets, addition is commutative, i.e. $a + b = b + a$ for all pairs a and b of elements.

Multiplication in our Examples

- The multiplication is commutative in all these examples except for $M_2(\mathbb{R})$. For 2×2 matrices A and B, the products AB and BA need not be equal.

- Except for $2\mathbb{Z}$ 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. The integer 1
  2. The rational number 1
  3. The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
  4. No identity element for multiplication
  5. The function $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 1$ for all $x \in \mathbb{R}$
  6. The polynomial 1
  7. The congruence class $\bar{1}$ modulo 6

- 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. All the other examples contain non-zero elements without multiplicative inverses.

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

1.2 The Axioms of a Ring

NOTE: In this section and throughout these lecture notes, please do not confuse the symbol R, which is used for a general ring, with the symbol $\mathbb{R}$ which is used for the set of real numbers.

Definition 1.2.1 *A* ring *is a non-empty set* R *equipped with two binary operations called addition* $(+)$ *and multiplication* $(\times)$*, satisfying the following properties :*

The first four are concerned with the operation that is called addition.

A1 Addition is associative.
$(r+s)+t = r+(s+t)$ for all $r, s, t \in R$.

A2 Addition is commutative. $r+s = s+r$ for all $r, s \in R$.

A3 R contains an identity element for addition, denoted by 0_R and called the *zero element* of R.
$r + 0_R = 0_R + r = r$ for all $r \in R$.

A4 Every element of R has an inverse with respect to addition. (The additive inverse of r is often denoted by $-r$).
For every $r \in R$, there exists an element $-r \in R$ for which $r + (-r) = 0_R$.

NOTE : Axioms A1 to A4 could be summarized by saying that R is an abelian group under addition. (If this remark is not helpful for you, disregard it for now).

The multiplication operation is required only to satisfy one special condition :

M1 Multiplication is associative.
$(r \times s) \times t = r \times (s \times t)$ for all $r, s, t \in R$.

The last two axioms are concerned with the manner in which the two operations must interact.

D1 $r \times (s+t) = (r \times s) + (r \times t)$ for all $r, s, t \in R$.

D2 $(r+s) \times t = (r \times t) + (s \times t)$ for all $r, s, t \in R$.
-Distributive laws for multiplication over addition.

REMARKS

1. A ring is called *commutative* if its multiplication is commutative.

2. A ring R is called *unital* or referred to as a *ring with identity* if it contains an identity element for multiplication. In this case we will denote the multiplicative identity by 1_R or just 1. We have already met one example of a ring without identity, namely the ring $2\mathbb{Z}$ of *even integers*.

3. The term "ring" was introduced by David Hilbert in the late 19th century, when he referred to a "Zahlring" or "number ring".

Our first theorem about rings is the following consequence of the ring axioms.

Theorem 1.2.2 *Let R be a ring. Then for all elements r of R we have*

$$0_R \times r = 0_R \text{ and } r \times 0_R = 0_R.$$

i.e. multiplying any element of R by the zero element results in the zero element as the product.

Proof : Let $r \in R$. We have

$$\begin{aligned}(0_R \times r) + (0_R \times r) &= (0_R + 0_R) \times r \\ &= 0_R \times r.\end{aligned}$$

Adding the additive inverse of the element $0_R \times r$ to both sides of this equation gives

$$0_R \times r = 0_R.$$

A similar argument shows that $r \times 0_R = 0_R$. □

THREE REMARKS

1. The problem of deducing the truth of a statement like Theorem 1.2.2 from the axioms of a ring might be somewhat daunting. The proof may not be too hard to follow, but could you have come up with it yourself? If you were trying to, and you didn't know where to start, there are certain observations you could make that might help. There are nine axioms for rings - which might be likely to be helpful in proving the two (left and right) statements of Theorem 1.2.2? Well, the statement is about multiplication and about the zero element. According to the ring axioms, what is special about the zero element has to do with addition not multiplication. So it might seem likely that the statement in the theorem is essentially connected to the interaction of the addition and multiplication - the two axioms that deal with that are the *distributive laws*, so maybe we should not be so surprised that these have a crucial role in the proof.

2. The next two remarks are about the philosophy of abstract algebra and the mechanisms by which the subject progresses. The definition of a ring consists of a list of technical properties, but the motivation for this definition is the ubiquity of objects having these properties, like the ones in Section 1.1. When making a definition like that of a ring (or group or vector space), the goal is to arrive at a set of axioms that exactly captures the crucial unifying properties of those objects that you wish to study. In familiar number systems like the integers, the rational numbers and the real numbers, we are all used to the fact with which Theorem 1.2.2 is concerned, namely that "multiplying by zero gives zero". The same fact is easily observed to hold in the polynomial ring $\mathbb{Q}[x]$ and in the ring of matrices $M_2(\mathbb{R})$. We might well speculate that in any ring, it is probably the case that multiplying by the zero element always results in the zero element. But before we can assume that this property holds in *every ring* and incorporate it into our mental scheme for thinking about rings we must *deduce this property as a consequence of the ring axioms*.

   If we were unable to do this, but we only wanted to study rings with the property described in Theorem 1.2.2, we could an extra axiom to our definition of a ring insisting on this "multiplication by zero" property. However the fact that this property *does* turn out to follow from the standard ring axioms means that it does not need to be included in the definition.

3. On looking at Definition 1.2.1, you may wonder why these nine axioms in particular are chosen to comprise the definition of a ring. Does it look like an arbitrary selection of rules? Why do we insist that the addition have an identity element and that every element have an inverse for addition, but where the multiplication is concerned only ask that it be associative? What happens if we add more axioms about how the multiplication should behave, or drop some of the axioms about addition? The answer is that people do these things and they lead to different areas of study within abstract algebra. Relaxing the addition axioms in various ways leads to different types of algebraic structures such as *near–rings* and *semirings*. If you drop the requirement that multiplication must be associative then you are studying *non-associative rings* – people do study all of these variants and some of them have important connections to other areas of mathematics. You can even relax the distributive laws and people do this too. However *rings* themselves as defined in Definition 1.2.1 are of paramount importance in mathematics.

   On the other hand, if you want more instead of fewer axioms, you can insist that multiplication be commutative as well as associative, then you are studying *commutative rings*. In fact much of this course will be concerned with commutative rings. If you further insist that you want an identity element for multiplication and that every (non-zero) element have an inverse for multiplication, then you are studying *fields*. Fields are examples of rings, and field theory itself is a vast area of mathematical activity. A crucial practice in studying abstract algebra is to be absolutely clear on the precise axioms that determine the class of objects that you are studying.

1.3 Units in Rings

As we have already mentioned, the axioms of a ring are not very restrictive concerning how the operation of multiplication should behave - all we ask is that it should be associative. We do not even insist that every ring should contain an identity element for multiplication (although incidentally some authors in ring theory do). If a ring does contain an identity element for multiplication, then we can enter a discussion about whether or not something like *division* is possible in the ring; we can try to identify pairs of elements that are related to each other in the way that a rational number is related to its reciprocal or in the way that a non-singular matrix is related to its inverse.

Definition 1.3.1 *Let R be a ring with identity element 1_R for multiplication. An element $r \in R$ is called a* unit *in R if there exists $s \in R$ for which*

$$r \times s = 1_R \text{ and } s \times r = 1_R.$$

In this case r and s are (multiplicative) inverses of each other.

Example 1.3.2

1. In $\mathbb{Q}$ every element except 0 is a unit; the inverse of a non-zero rational number is its reciprocal.
2. In $\mathbb{Z}$ the only units are 1 and -1 : no other integer can be multiplied by an integer to give 1.
3. In $M_2(\mathbb{R})$, the units are the 2×2 matrices with non-zero determinant, and the identity element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
4. In $\mathbb{Z}/6\mathbb{Z}$ the only units are $\bar{1}$ and $\bar{5}$; each of these is its own inverse.
5. Question for discussion in the seminar : *what are the units in $M_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries?*

NOTATION: We will denote the set of units in a ring R with identity by $\mathcal{U}(R)$.

REMARKS

1. If R is a unital ring having two or more elements then it follows from Theorem 1.2.2 that the zero element of R and the multiplicative identity in R cannot be the same element.
2. If R has two or more elements then 0_R cannot be a unit in R, again by Theorem 1.2.2.

3. It is possible for a ring to have only one element; for example the subset of $\mathbb{Z}$ containing only 0 is a ring. (This is called the zero ring and as an example of a ring it is not very instructive)

4. 1_R is always a unit in R since it is its own inverse.

The next theorem is concerned with a special property of the subset of a ring consisting of the units. Suppose that R is a unital ring. Then from the above comments it follows that $\mathcal{U}(R)$ is a subset of R that includes the (multiplicative) identity element but not the zero element. Is $\mathcal{U}(R)$ just a set, or does it have algebraic structure of its own? The full ring R has addition and multiplication defined on it. If we take two units of R we can add them in R; will the result be a unit? If we take two units of R and multiply them (in R), will the result be a unit? If the answer to this second question is yes, then the set of units of R is itself an algebraic structure with respect to the multiplication of R, and we can study its properties.
Algebraists are always on the lookout for substructures of the objects that they are studying, which are themselves algebraic structures with respect to the operation(s) of the larger object. The general thinking behind this practice is that small things are usually easier to understand than big things, and that we have some chance of understanding (at least partically) a large complicated algebraic structure if we can identify smaller parts of it that are themselves algebraic structures.

Theorem 1.3.3 *Let R be a ring with identity element 1_R. Then $\mathcal{U}(R)$ is a group under the multiplication of R. ($\mathcal{U}(R)$ is called the unit group of R).*

Note : The statement that $\mathcal{U}(R)$ is a group under multiplication means that :

- $\mathcal{U}(R)$ is *closed* under multiplication - whenever elements a and b belong to $\mathcal{U}(R)$, so does their product ab.
- $\mathcal{U}(R)$ contains an identity element for multiplication.
- $\mathcal{U}(R)$ contains a multiplicative inverse for each of its elements.

Proof of Theorem 1.3.3: We need to show

1. $\mathcal{U}(R)$ is closed under the multiplication of R; i.e. that rs is a unit in R whenever r and s are units in R. So assume that r and s belong to $\mathcal{U}(R)$ and let r^{-1} and s^{-1} denote their respective inverses in R. Then

$$\begin{aligned}(rs)(s^{-1}r^{-1}) &= r(ss^{-1})r^{-1}\\ &= r1_Rr^{-1}\\ &= rr^{-1}\\ &= 1_R.\end{aligned}$$

Similarly $(s^{-1}r^{-1})(rs) = 1_R$ and so $s^{-1}r^{-1}$ is an inverse in R for rs, and $rs \in \mathcal{U}(R)$.

2. $\mathcal{U}(R)$ contains an identity element for multiplication. This is true since $1_R \in \mathcal{U}(R)$.

3. $\mathcal{U}(R)$ contains an inverse for each of its elements.
   To see this, suppose $r \in \mathcal{U}(R)$, and let r^{-1} be the inverse of r in R. Then $r^{-1}r = 1_R$ and $rr^{-1} = 1_R$, so r is the inverse of r^{-1}, and r^{-1} is in $\mathcal{U}(R)$.

This proves the theorem. □

EXAMPLES

1. $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$ is a cyclic group of order 2.

2. The unit group of the matrix ring $M_n(\mathbb{R})$ is the general linear group $GL(n, \mathbb{R})$ of $n \times n$ invertible matrices over $\mathbb{R}$.

3. The unit group of $\mathbb{Q}$ is denoted $\mathbb{Q}^\times$ and consists of all non-zero rational numbers.

QUESTION FOR DISCUSSION IN THE SEMINAR: *In general, is there anything to be said about the behaviour of* $\mathcal{U}(R)$ *with respect to addition in* R*?*

Suppose that R is a ring with identity. Then we know that the unit group of R cannot include the zero element of R, but any non-zero element of R could potentially be a unit. A particularly nice thing to happen is for *every* non-zero element of R to be a unit. Rings in which this occurs are worthy of special study.

Definition 1.3.4 *A ring with identity is called a* field *if it is commutative and every non-zero element is a unit (so we can divide by every non-zero element).*

Examples of fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}/5\mathbb{Z}$ (check).

A ring with identity in which every non-zero element is a unit is called a *division ring*. Commutative division rings are fields. Examples of non-commutative division rings are not easy to find, but we will see at least one in this course.

1.4 Integral Domains and Zero–Divisors

We saw in Theorem 1.2.2 that whenever an element of a ring is multiplied by zero, the result is zero. When working in the set of real numbers we often use the converse of this - a product ab can be zero in $\mathbb{R}$ only if at least one of a and b is equal to zero.
QUESTION FOR THE SEMINAR: *When/how do we use this?*

QUESTION: Is it true in every ring that the product of two elements can be zero only if at least one of the elements is zero? To think about this question, look at some examples.

Example 1.4.1 1. *In* $M_2(\mathbb{Q})$

$$\begin{pmatrix} 1 & -1 \\ -2 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

i.e. the product of two non-zero matrices in $M_2(\mathbb{Q})$ *can be the zero matrix.*

2. *In* $\mathbb{Z}/6\mathbb{Z}$, $\bar{2} \times \bar{3} = \bar{0}$

So the answer to the question is no in general. However, it *is* of interest to study the class of rings in which the property described in the question holds.

Definition 1.4.2 *Let* R *be a ring with zero element* 0_R. *An element* a *of* R *is called a* (left) zero–divisor *in* R *if* $a \neq 0_R$ *and there exists an element* $b \neq 0_R$ *of* R *for which* $ab = 0_R$. *(In this case* b *is a right zero–divisor).*

NOTE: If R is commutative then $ab = ba$ and we just talk about zero–divisors (not left and right zero–divisors).

Definition 1.4.3 *A commutative ring with identity that contains no zero-divisors is called an* integral domain *(or just a domain).*

In an integral domain, the product of two elements can be zero only if one of the elements is zero.

EXAMPLES

1. $\mathbb{Z}$ is an integral domain. Somehow it is the "primary" example - it is from the ring of integers that the term "integral domain" is derived. The adjective "integral" in this context is related to "integer" (nothing to do with integrals in the calculus sense!).

2. Every *field* is an integral domain. For let F be a field and suppose that a, b are elements of F for which $ab = 0_F$. Assume $a \neq 0$. Then a has a multiplicative inverse in F and

$$\begin{aligned} ab &= 0_F \\ \Longrightarrow a^{-1}(ab) &= a^{-1}0_F \\ \Longrightarrow (a^{-1}a)b &= 0_F \text{ by Theorem 1.2.2} \\ \Longrightarrow 1_F b &= 0_F \\ \Longrightarrow b &= 0_F. \end{aligned}$$

   REMARK: It follows from the above argument that no unit can be a (left or right) zero-divisor in any ring.

   EXERCISE: Write down a proof of the statement of the above remark.

3. An example of a commutative ring with identity that is not an integral domain is $\mathbb{Z}/6\mathbb{Z}$ (or $\mathbb{Z}/n\mathbb{Z}$ for any composite natural number n).

QUESTIONS FOR THE SEMINAR:

1. *For which natural numbers n is $\mathbb{Z}/n\mathbb{Z}$ a field?*
2. *For which natural numbers n is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?*
3. *For a natural number n, which elements of $\mathbb{Z}/n\mathbb{Z}$ are units?*
4. *Is it true for every natural number n that every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero-divisor? Can we prove this?*
5. *Suppose that R is a commutative ring with identity that is not an integral domain. Must it be true that every non-zero element of R is either a zero-divisor or a unit?*