1. Introduction to commutative rings and fields

Very informally speaking, a commutative ring is a set in which we can add, subtract and multiply elements so that the "usual laws" hold. A field is a commutative ring in which we can also perform division (again satisfying the "usual laws").

Based on this description, we would expect that the familiar 'number systems' $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers) and $\mathbb{C}$ (complex numbers) are all commutative rings, and among those $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, while $\mathbb{Z}$ is not a field (we cannot divide in $\mathbb{Z}$, as the quotient of two integers is not necessarily an integer, so we cannot perform division within the original set).

In order to justify the above claim, we need to give formal definitions of commutative rings and fields, for which we need to say what we mean by the "usual laws" of arithmetic operations. It is impossible to write down all possible valid laws, but there is also no need to do that. What we want to do is to declare the list of basic laws called *axioms*, so that all other laws would follow from them.

1.1. **Axioms for arithmetic operations.** Below R stands for one of the four sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. We start with axioms of addition:

- (A0) R is closed under $+$, that is, if $x, y \in R$, then $x + y \in R$
- (A1) $+$ is commutative, that is, $x + y = y + x$ for all $x, y \in R$
- (A2) $+$ is associative, that is, $x + (y + z) = (x + y) + z$ for all $x, y, z \in R$
- (A3) There exists $0 \in R$ such that $x + 0 = 0 + x = x$ for all $x \in R$
- (A4) For any $x \in R$ there exists $-x$ in R such that $x + (-x) = (-x) + x = 0$. Such an element $-x$ is called *an additive inverse of* x. Thus, (A4) says that every $x \in R$ has an additive inverse in R.

Remark: It is easy to deduce from these axioms that for every $x \in R$ there is *unique* element $-x$ satisfying (A4). This ensures that notation $-x$ is unambiguous ($-x$ is uniquely determined by x) and also that we can talk about 'THE additive inverse'.

Once we introduced additive inverses, we can define subtraction in terms of addition by setting

$$x - y = x + (-y) \text{ for all } x, y \in R.$$

Next we state axioms of multiplication (denoted by $\cdot$):

(M0) R is closed under $\cdot$, that is, if $x, y \in R$, then $x \cdot y \in R$

(M1) $\cdot$ is commutative, that is, $x \cdot y = y \cdot x$ for all $x, y \in R$

(M2) $\cdot$ is associative, that is, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in R$

(M3) There exists $1 \in R$ (often called the *unity of* R) such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in R$

(M4) For every NONZERO $x \in R$ there exists x^{-1} in R such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Such an element x^{-1} is called *the multiplicative inverse of* x (as with additive inverses, one can show that x^{-1} is unique). Thus, (M4) says that every nonzero $x \in R$ has a multiplicative inverse in R.

Note that (M0)-(M3) hold in all the examples we considered so far, while (M4) holds in $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, but does not hold in $\mathbb{Z}$ (for instance $2 \in \mathbb{Z}$, but $2^{-1} \notin \mathbb{Z}$).

Finally, there are two axioms, relating addition and multiplication, called the distributivity laws:

(D1) $(x + y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in R$

(D2) $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in R$.

Remark: Of course, if (M1) holds in R, then (D1) and (D2) are equivalent (so we only need to require one of these axioms). The reason we list both (D1) and (D2) explicitly is that there are important algebraic structures where (M1) does not hold, but both (D1) and (D2) do hold.

Definition. Let R be a set with two operations $+$ and $\cdot$. Then

(i) R is called a *ring* if it satisfies axioms (A0)-(A4), (M0),(M2) and (D1)-(D2)

(i) R is called a *commutative ring* if R is a ring which also satisfies (M1) (thus, the word 'commutative' refers to commutativity of multiplication). Equivalently, R is a commutative ring if it satisfies axioms (A0)-(A4), (M0)-(M2) and (D1)-(D2)

(iii) R is called a *ring with* 1 if R is a ring which also satisfies (M3). Equivalently, R is a ring with 1 if it satisfies axioms (A0)-(A4), (M0), (M2), (M3) and (D1)-(D2)

(iv) R is called a *commutative ring with* 1 if R is both a commutative ring and a ring with 1. Equivalently, R is a commutative ring with 1 if it satisfies axioms (A0)-(A4), (M0)-(M3) and (D1)-(D2)

(v) R is called a *field* if R is a commutative ring with 1 which satisfies (M4) (so every nonzero element is invertible) and in addition $0 \neq 1$.

Equivalently, R is a field if it satisfies all of the 12 axioms above and $0 \neq 1$.

Thus, according to our definition, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are indeed fields, and $\mathbb{Z}$ is a commutative ring with 1 which is not a field. A simple example of a commutative ring without 1 is $2\mathbb{Z}$ (even integers). Finally, an example of a non-commutative ring is $Mat_2(\mathbb{R})$, two by two matrices with real entries.

The above definition is completely formal, provided one interprets correctly the word 'operation' in it. Here we are talking about *binary operations* on a set, which can be defined as follows.

Definition. Let X be an arbitrary set. A *binary operation* on X is a rule (denoted by some symbol, say, $*$) which to every ordered pair (x, y) of elements of X associates another element of X denoted by $x * y$.

The main point of this definition is that for every $x, y \in X$, the element $x * y$ should again lie in X and should be uniquely determined by x and y.

A more formal way to define the notion of a binary operation is as follows:

Definition. A *binary operation* $*$ on X is a function $* : X \times X \to X$ where $X \times X = \{(x, y) : x, y \in X\}$ is the set of ordered pairs of elements of X.

Remark: Note that by saying that $+$ and $\cdot$ are binary operations on R we already require that axioms (A0) and (M0) must hold. Thus, formally those axioms do not have to appear on the list. It is, however, a good idea to keep them, as if we want to check that some set R is a ring with respect to some operations $+$ and $\cdot$, then we do have to check those properties.

We now give a few examples showing how to derive additional properties of arithmetic operations in rings from axioms. In all example below R denotes a commutative ring.

Example 1.1. *Prove that $a + (b + c) = c + (b + a)$ for all $a, b, c \in R$.*
Proof:

$$\begin{array}{lll} a + (b + c) & = a + (c + b) & \text{by (A1)} \\ & = (c + b) + a & \text{by applying (A1) with } x = a \text{ and } y = c + b \\ & = c + (b + a) & \text{by (A2).} \end{array}$$

Example 1.2. *(Cancellation law for addition) Suppose that $x + z = y + z$ for some $x, y, z \in R$. Prove that $x = y$.*
Proof: Here we are given a different type of problem – we have to deduce one equality from another one, so we have to make sure that we do things in correct order. We have to start with what we are given ($x + z = y + z$) and

then use axioms to deduce what we want ($x = y$). It may be tempting to do things in reverse order (start with $x = y$ and deduce that $x + z = y + z$), but that would not give a valid proof.

Intuitively, it is clear what we should do: start with $x + z = y + z$ and then subtract z from both sides. However, since our axioms do not explicitly use subtraction, we have to proceed in several steps.

$x + z = y + z$	This is what we are given
$(x + z) + (-z) = (y + z) + (-z)$	Add $-z$ to both sides on the right
$x + (z + (-z)) = y + (z + (-z))$	Use (A2) on both sides
$x + 0 = y + 0$	Use (A4) on both sides
$x = y$	Use (A3) on both sides

Remark: Note that in the first step we use the following property without justification: *if we have some equality, then we can add the same element to both sides of that equality (that is, if $a = b$, then $a + c = b + c$).* Such a transition is always valid, but it is important to understand why it is valid. In order to justify it, we need to go back to the definition of a binary operation. Since $+$ is a binary operation, the element $a + c$ is completely determined by the ordered pair (a, c); at this point, it may be useful to write $+(a, c)$ (thinking of $+$ as a function) instead of $a + c$. Since $a = b$, the ordered pairs (a, c) and (b, c) are the same (since they have the same first component and the same second component). Hence the result of applying the binary operation $+$ should by the same: $+(a, c) = +(b, c)$ or, in usual notations, $a + c = b + c$.

Example 1.3. *Prove that $x \cdot 0 = 0$ for all $x \in R$.*
Proof: Here we start with a trick: $x \cdot 0 = x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$ using (A3) and (D). On the other hand, again by (A3), we have $x \cdot 0 = 0 + (x \cdot 0)$.

Combining these two equalities, we get $(x \cdot 0) + (x \cdot 0) = x \cdot 0 = 0 + (x \cdot 0)$, so applying the cancellation law (the result of the previous exercise), we deduce that $x \cdot 0 = 0$.

Example 1.4. *Prove that $(-1) \cdot x = -x$ for all $x \in R$.*

We will start by giving a wrong proof presented below:

$(-1) \cdot x$	$=$	$-x$	
$((-1) \cdot x) + x$	$=$	$(-x) + x$	add x to both sides
$(-1 \cdot x) + 1 \cdot x$	$=$	0	use (M3) on the left
$((-1) + 1) \cdot x$	$=$	0	use (D) on the left
$0 \cdot x$	$=$	0	use (A4) on the left

The last line is true by Example 1.3, and we would like to say that we are done. This argument is wrong because we did steps in the wrong order – we started with what we had to prove and deduced something which we already

know is true. However, this does not mean that the above computation is useless, for if we are able to reverse all the steps, we will get a legitimate proof.

A quick glance through the argument shows that all the steps can indeed be reversed. In fact, for most steps even justification remains the same - the only exception is that instead of adding x to both sides in the first step, we will be using cancellation law (in what will now be the last step). Thus, reversing the steps, we obtain what is now a legitimate proof.

$$\begin{array}{rcll} 0 \cdot x & = & 0 & \text{true by the previous example} \\ & \Downarrow & & \\ ((-1)+1) \cdot x & = & 0 & \text{use (A4) on the left} \\ & \Downarrow & & \\ ((-1) \cdot x) + 1 \cdot x & = & 0 & \text{use (D) on the left} \\ & \Downarrow & & \\ ((-1) \cdot x) + x & = & (-x) + x & \text{use (M3) on the left} \\ & \Downarrow & & \\ (-1) \cdot x & = & -x & \text{use cancellation law} \end{array}$$

1.2. **Book references.** The material of this lecture is covered in [Gilbert, 2.1]. The formal point of view there is different, as Gilbert only discusses axioms of integers and does not talk about rings and fields (in 2.1); however, the logic in all the examples remains the same.

Pinter introduces rings and fields in Chapter 17. It may be a bit hard to read at this point as many of the ring-theoretic notions are defined using group-theoretic terminology.