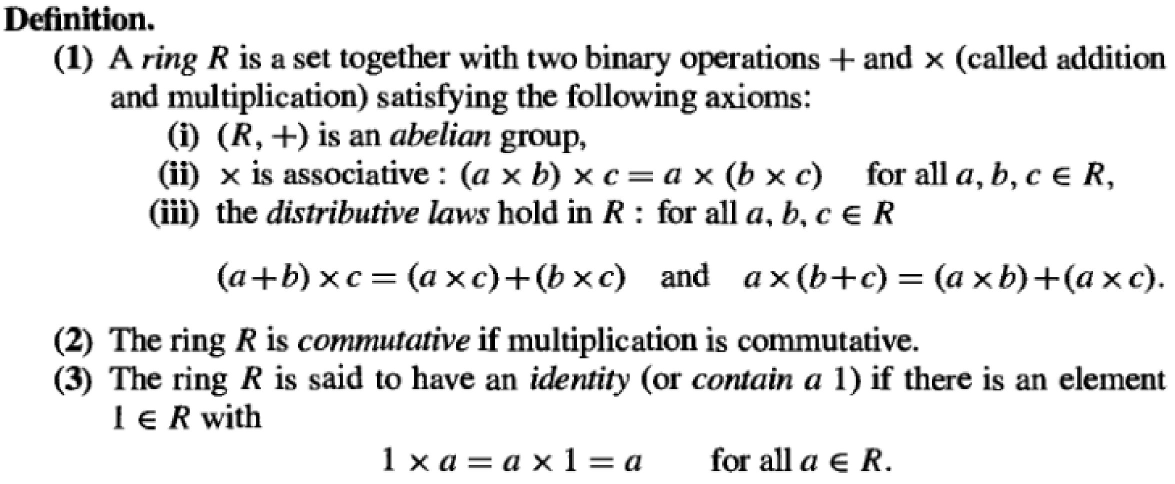
Reading Assignment 7
Lecture 21

1. Watch the following video about the definition of Ring.
   Ring Definition
2. Read the content below.



Definition.

(1) A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

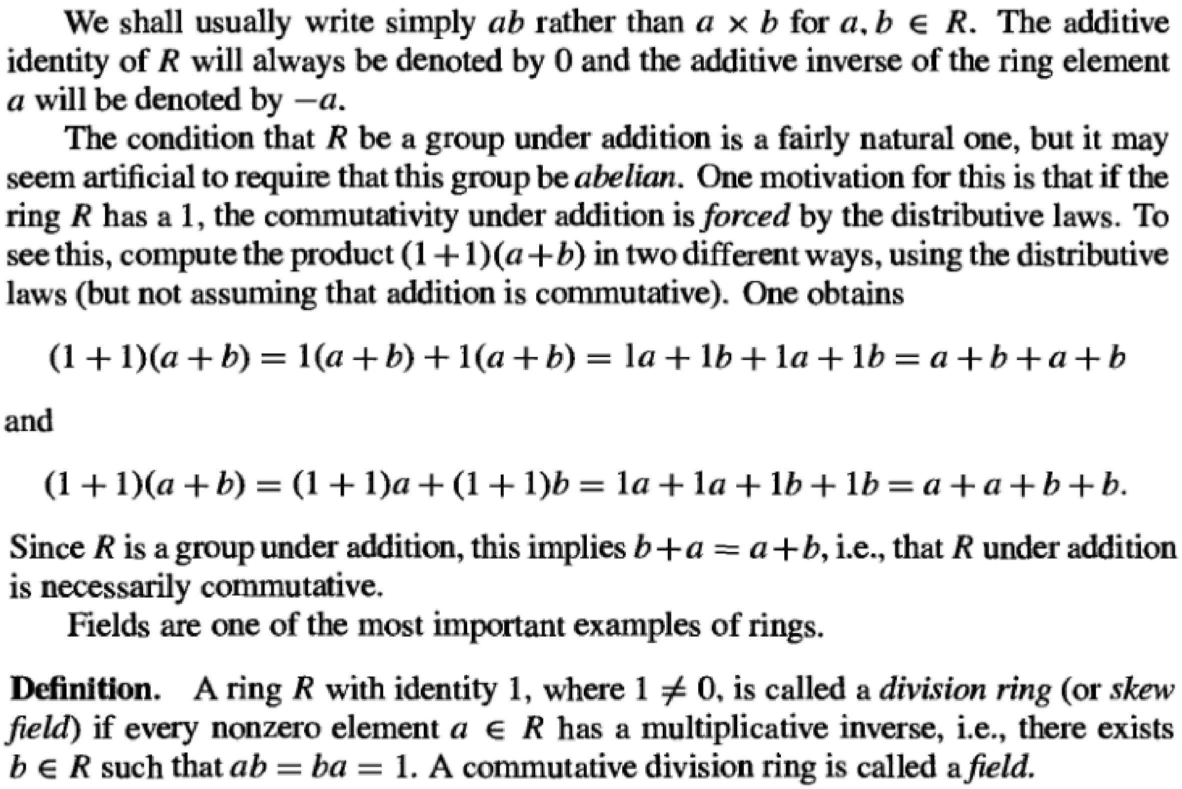
- **(i)** $(R, +)$ is an *abelian* group,
- **(ii)** $\times$ is associative : $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,
- **(iii)** the *distributive laws* hold in R : for all $a, b, c \in R$

$$(a+b) \times c = (a \times c)+(b \times c) \quad \text{and} \quad a \times (b+c) = (a \times b)+(a \times c).$$

(2) The ring R is *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain a* 1) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \qquad \text{for all } a \in R.$$



We shall usually write simply ab rather than $a \times b$ for $a, b \in R$. The additive identity of R will always be denoted by 0 and the additive inverse of the ring element a will be denoted by $-a$.

The condition that R be a group under addition is a fairly natural one, but it may seem artificial to require that this group be *abelian*. One motivation for this is that if the ring R has a 1, the commutativity under addition is *forced* by the distributive laws. To see this, compute the product $(1+1)(a+b)$ in two different ways, using the distributive laws (but not assuming that addition is commutative). One obtains

$$(1+1)(a+b) = 1(a+b) + 1(a+b) = 1a + 1b + 1a + 1b = a + b + a + b$$

and

$$(1+1)(a+b) = (1+1)a + (1+1)b = 1a + 1a + 1b + 1b = a + a + b + b.$$

Since R is a group under addition, this implies $b+a = a+b$, i.e., that R under addition is necessarily commutative.

Fields are one of the most important examples of rings.

Definition. A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

Examples

(1) The simplest examples of rings are the ***trivial rings*** obtained by taking R to be any commutative group (denoting the group operation by $+$) and defining the multiplication $\times$ on R by $a \times b = 0$ for all $a, b \in R$. It is easy to see that this multiplication defines a commutative ring. In particular, if $R = \{0\}$ is the trivial group, the resulting ring R is called the *zero ring*, denoted $R = 0$. Except for the zero ring, a trivial ring does not contain an identity ($R = 0$ is the only ring where $1 = 0$; we shall often exclude this ring by imposing the condition $1 \neq 0$). Although trivial rings have two binary operations, multiplication adds no new structure to the additive group and the theory of rings gives no information which could not already be obtained from (abelian) group theory.

(2) The ring of integers, $\mathbb{Z}$, under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1). The ring axioms (as with the additive group axioms) follow from the basic axioms for the system of natural numbers. Note that under ***multiplication*** $\mathbb{Z}-\{0\}$ is ***not*** a group (in fact, there are very few multiplicative inverses to elements in this ring). We shall come back to the question of these inverses shortly.

(3) Similarly, the rational numbers, $\mathbb{Q}$, the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$, are commutative rings with identity (in fact they are fields). The ring axioms for each of these follow ultimately from the ring axioms for $\mathbb{Z}$. We shall verify this when we

(4) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element $\bar{1}$) under the operations of addition and multiplication of residue classes (frequently referred to as "modular arithmetic"). We saw that the additive abelian group axioms followed from the general principles of the theory of quotient groups (indeed this was the prototypical quotient group). We shall shortly prove that the remaining ring axioms (in particular, the fact that multiplication of residue classes is well defined) follow analogously from the general theory of quotient rings.

In all of the examples so far the rings have been commutative. Historically, one of the first noncommutative rings was discovered in 1843 by Sir William Rowan Hamilton (1805–1865). This ring, which is a division ring, was extremely influential in the subsequent development of mathematics and it continues to play an important role in certain areas of mathematics and physics.

(5) (The ***(real) Hamilton Quaternions***) Let $\mathbb{H}$ be the collection of elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ are real numbers (loosely, "polynomials in $1, i, j, k$ with real coefficients") where addition is defined "componentwise" by

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k$$

and multiplication is defined by expanding $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$ using the distributive law (being careful about the order of terms) and simplifying using the relations

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

(where the real number coefficients commute with i, j and k). For example, The fact that $\mathbb{H}$ is a ring may be proved by a straightforward, albeit lengthy, check of the axioms (associativity of multiplication is particularly tedious). The Hamilton Quaternions are a noncommutative ring with identity ($1 = 1+0i+0j+0k$). Similarly, one can define the ring of *rational* Hamilton Quaternions by taking a, b, c, d to be rational numbers above. Both the real and rational Hamilton Quaternions are *division rings*, where inverses of nonzero elements are given by

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}.$$

(6) One important class of rings is obtained by considering rings of functions. Let X be any nonempty set and let A be any ring. The collection, R, of all (set) functions $f : X \to A$ is a ring under the usual definition of pointwise addition and multiplication of functions: $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$. Each ring axiom for R follows directly from the corresponding axiom for A. The ring R is commutative if and only if A is commutative and R has a 1 if and only if A has a 1 (in which case the 1 of R is necessarily the constant function 1 on X).

If X and A have more structure, we may form other rings of functions which respect those structures. For instance, if A is the ring of real numbers $\mathbb{R}$ and X is the closed interval $[0, 1]$ in $\mathbb{R}$ we may form the ring of all *continuous* functions from $[0, 1]$ to $\mathbb{R}$ (here we need basic limit theorems to guarantee that sums and products of continuous functions are continuous) — this is a commutative ring with 1.

(7) An example of a ring which does not have an identity is the ring $2\mathbb{Z}$ of even integers under usual addition and multiplication of integers (the sum and product of even integers is an even integer).

Proposition 1. Let R be a ring. Then

(1) $0a = a0 = 0$ for all $a \in R$.

(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a).

(3) $(-a)(-b) = ab$ for all $a, b \in R$.

(4) if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof: These all follow from the distributive laws and cancellation in the additive group R. For example, (1) follows from $0a = (0+0)a = 0a+0a$. The equality $(-a)b = -(ab)$ in (2) follows from $ab + (-a)b = (a+(-a))b = 0b = 0$. The rest follow similarly and are left to the reader.

This proposition shows that because of the distributive laws the additive and multiplicative structures of a ring behave well with respect to one another, just as in the familiar example of the integers.