Math 250
Burger

Definitions: Rings, Groups and Fields

A **group** is a set, G, together with an operation • (called the **group law** of G) that combines any two elements a and b to form another element, denoted $a \bullet b$ or ab. To qualify as a group, the set and operation, $(G, \bullet)$, must satisfy four requirements known as the **group axioms**:[4]

Closure

For all a, b in G, the result of the operation, $a \bullet b$, is also in G.[b]

Associativity

For all a, b and c in G, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

Identity element

There exists an element e in G, such that for every element a in G, the equation $e \bullet a = a \bullet e = a$ holds. The identity element of a group G is often written as 1 or 1_G,[5] a notation inherited from the multiplicative identity.

Inverse element

For each a in G, there exists an element b in G such that $a \bullet b = b \bullet a = 1_G$.

The order in which the group operation is carried out can be significant. In other words, the result of combining element a with element b need not yield the same result as combining element b with element a; the equation

$$a \bullet b = b \bullet a$$

may not always be true. This equation does always hold in the group of integers under addition, because $a + b = b + a$ for any two integers (commutativity of addition). However, it does not always hold in the symmetry group below. Groups for which the equation $a \bullet b = b \bullet a$ always holds are called *abelian* (in honor of Niels Abel).

A **ring** is a set R equipped with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ (where × denotes the Cartesian product), called *addition* and *multiplication*. To qualify as a ring, the set and two operations, $(R, +, \cdot)$, must satisfy the following requirements known as the *ring axioms*.[4]

- $(R, +)$ is required to be an *abelian group* under addition:

1. Closure under addition.	For all a, b in R, the result of the operation $a + b$ is also in R.[c]
2. Associativity of addition.	For all a, b, c in R, the equation $(a + b) + c = a + (b + c)$ holds.
3. Existence of additive identity.	There exists an element 0 in R, such that for all elements a in R, the equation $0 + a = a + 0 = a$ holds.
4. Existence of additive inverse.	For each a in R, there exists an element b in R such that $a + b = b + a = 0$
5. Commutativity of addition.	For all a, b in R, the equation $a + b = b + a$ holds.

- (R, ·) is required to be a monoid under multiplication:

1.	Closure under multiplication.	For all a, b in R, the result of the operation $a \cdot b$ is also in R.[c[›]]
2.	Associativity of multiplication.	For all a, b, c in R, the equation $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds.
3.	Existence of multiplicative identity.[a[›]]	There exists an element *1* in R, such that for all elements a in R, the equation $1 \cdot a = a \cdot 1 = a$ holds.

- The distributive laws:

1. For all a, b and c in R, the equation $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ holds.
2. For all a, b and c in R, the equation $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ holds.

This definition assumes that a binary operation on R is a function defined on $R \times R$ with values in R. Therefore, for any a and b in R, the addition $a + b$ and the product $a \cdot b$ are elements of R.

The most familiar example of a ring is the set of all integers, $\mathbf{Z} = \{..., −4, −3, −2, −1, 0, 1, 2, 3, 4, ... \}$, together with the usual operations of addition and multiplication.[3]

Intuitively, a **field** is a set F that is a commutative group with respect to two compatible operations, addition and multiplication, with "compatible" being formalized by *distributivity*, and the caveat that the additive identity (0) has no multiplicative inverse (one cannot divide by 0).

The most common way to formalize this is by defining a *field* as a set together with two operations, usually called *addition* and *multiplication*, and denoted by + and ·, respectively, such that the following axioms hold; *subtraction* and *division* are defined implicitly in terms of the inverse operations of addition and multiplication:[note 1]

Closure of F under addition and multiplication

For all a, b in F, both $a + b$ and $a \cdot b$ are in F (or more formally, + and · are binary operations on F).

Associativity of addition and multiplication

For all a, b, and c in F, the following equalities hold: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Commutativity of addition and multiplication

For all a and b in F, the following equalities hold: $a + b = b + a$ and $a \cdot b = b \cdot a$.

Additive and multiplicative *identity*

There exists an element of F, called the *additive identity* element and denoted by 0, such that for all a in F, $a + 0 = a$. Likewise, there is an element, called the *multiplicative identity* element and denoted by 1, such that for all a in F, $a \cdot 1 = a$. To exclude the trivial ring, the additive identity and the multiplicative identity are required to be distinct.

Additive and multiplicative *inverses*

For every a in F, there exists an element $-a$ in F, such that $a + (-a) = 0$. Similarly, for any a in F other than 0, there exists an element a^{-1} in F, such that $a \cdot a^{-1} = 1$. (The elements $a + (-b)$ and $a \cdot b^{-1}$ are also denoted $a - b$ and a/b, respectively.) In other words, *subtraction* and *division* operations exist.

Distributivity of multiplication over addition

For all a, b and c in F, the following equality holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

A field is therefore an algebraic structure consisting of two abelian groups:

- F under $+$, $-$, and 0;
- $F \setminus \{0\}$ under $\cdot$, $^{-1}$, and 1, with $0 \neq 1$,

with $\cdot$ distributing over $+$.[1]