4. Some abstract algebra

As already observed the natural numbers are interesting as there are two natural operations on them, addition and multiplication. There are a bunch of obvious ways to improve the natural numbers. One way is to simply add the number 0 and consider the non-negative integers. If you add 0 to any number then nothing happens.

The annoying thing about the non-negative integers is that it is easy write down linear equations that don't always have solutions. There are no solutions to the equation

$$x + 2 = 1.$$

We have to include all negative numbers, so that we get the integers. The integers have the useful property that we can solve any equation of the form

$$x + a = b.$$

If $a < b$ the solution is a natural number, if $a = b$ the solution is zero and if $a > b$ the solution is a negative integer. A group is an abstract form of this situation.

Definition 4.1. *A **group** G is a set together with a **rule of multiplication***

$$\mu \colon G \times G \longrightarrow G.$$

Formally the product of two elements is $\mu(a, b)$, the result of applying the function μ to a and b. But as is customary, we we will use multiplicative notation:

$$\mu(a, b) = a \cdot b = ab.$$

Multiplication satisfies the following axioms:

(1) ***Associativity:*** *Multiplication is **associative**, that is,*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

for all a, b and $c \in G$.

(2) ***Identity:*** *There is an element $e \in G$ such that*

$$a \cdot e = a = e \cdot a.$$

for all $a \in G$.

(3) ***Inverses:*** *For every element $a \in G$ there is an element b such that*

$$a \cdot b = e = b \cdot a.$$

If in addition, we have

(4) ***Commutativity:*** *Multiplication is* ***commutative****, that is,*

$$a \cdot b = b \cdot a.$$

for all a, $b \in G$.

then we say that G *is* ***abelian****.*

Sets of number provide lots of examples of groups. The integers under addition is a group. Addition is well-known to be associative, 0 plays the role of the identity, the inverse of a is $-a$ and addition is commutative. In many abelian groups it is in fact customary to use additive notation rather than multiplicative notation.

Note that the rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers are all abelian groups under addition.

The natural numbers are not a group under addition. Addition is associative but there is no identity.

A ring is like a group but it captures the properties of addition and multiplication.

Definition 4.2. *A* ***ring*** R *is a set together with a* ***rule of addition*** *and a* ***rule of multiplication****:*

$$+ : G \times G \longrightarrow G \qquad \text{and} \qquad \cdot : G \times G \longrightarrow G.$$

$(R, +)$ *is an abelian group under addition, with* 0 *as the identity.*

Multiplication satisfies the following axioms:

(1) ***Associativity:*** *Multiplication is* ***associative****, that is,*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

for all a, b *and* $c \in R$.

(2) ***Identity:*** *There is an element* $1 \neq 0 \in R$ *such that*

$$a \cdot 1 = a = 1 \cdot a.$$

for all $a \in R$.

(3) ***Commutativity:*** *Multiplication is* ***commutative****, that is,*

$$a \cdot b = b \cdot a.$$

for all a, $b \in R$.

Addition and multiplication are compatible in the following sense:

(4) ***Distributivity:***

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

for all a, b *and* $c \in R$.

The integers are the quintessential example of a ring. The rationals, reals, and complex numbers are also rings.

Example 4.3. *The Gaussian integers are all complex numbers of the form $a + bi$, where a and b are integers.*

It is not hard to check that the Gaussian integers are a ring under addition and multiplication. In fact the key point is that the Gaussian integers are closed under addition, inverses and multiplication, which means if you add, take the inverse or multiply two Gaussian integers then you get a Gaussian integer.

Definition 4.4. *Let R be a ring. We say that R is an **integral domain** if whenever $ab = ac$ and $a \neq 0$ then $b = c$.*

The integers are an integral domain. The complex numbers are also an integral domain (in fact, just multiply by the inverse of a), so that the Gaussian integers are an integral domain.