

There are two common ways to build new mathematics: (1) take a common mathematical object or system and create an abstract version of it, trying to describe it as simply as possible and (2) take an already created object or system and add extra properties to make a new one.

For this section we will build a new system called a **field**. We can start with a known system: the real numbers  $\mathbb{R}$  with addition and multiplication. From previous study of algebra we know that addition and multiplication satisfy certain properties like the commutative law, the associative law and the distributive law. Then we create an abstract object that satisfies these properties (and others) but may not obviously satisfy all characteristics of the real numbers. Then we try and see what other properties we can derive. Another way to think about a field is to start with the idea of a set and then add some extra properties. Either way can have the following definition:

Definition: Let  $\mathbb{F}$  be a set and for elements  $a, b \in \mathbb{F}$  let there be two operations  $a + b$  and  $a \cdot b$ .  $(\mathbb{F}, +, \cdot)$  is a **field** if it satisfies the following 11 conditions (called the Field Axioms):

A1: For all  $a, b \in \mathbb{F}$ ,  $a + b \in \mathbb{F}$ . (Closure)

A2: For all  $a, b \in \mathbb{F}$ ,  $a + b = b + a$ . (Commutativity)

A3: For all  $a, b, c \in \mathbb{F}$ ,  $(a + b) + c = a + (b + c)$ . (Associativity)

A4: There exists an element called  $0 \in \mathbb{F}$  such that for all  $a \in \mathbb{F}$ ,  $a + 0 = a$ . (Existence of Additive Identity)

A5: For  $a \in \mathbb{F}$ , there exists an element  $-a \in \mathbb{F}$  such that  $a + -a = 0$ . (Existence of Additive Inverse)

M1: For all  $a, b \in \mathbb{F}$ ,  $a \cdot b \in \mathbb{F}$ . (Closure)

M2: For all  $a, b \in \mathbb{F}$ ,  $a \cdot b = b \cdot a$ . (Commutativity)

M3: For all  $a, b, c \in \mathbb{F}$ ,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ . (Associativity)

M4: There exists an element called  $1 \in \mathbb{F}$  with  $1 \neq 0$ , such that for all  $a \in \mathbb{F}$ ,  $a \cdot 1 = a$ . (Existence of Multiplicative Identity)

M5: For  $a \in \mathbb{F}$ ,  $a \neq 0$ , there exists an element  $a^{-1} \in \mathbb{F}$  such that  $a \cdot a^{-1} = 1$ . (Existence of Multiplicative Inverse)

D: For all  $a, b, c \in \mathbb{F}$ ,  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  (Distributivity)

---

Before we go on and use this definition, we should spend some time looking at its characteristics. First off, it is long, so each of the 11 conditions has been given a unique indicator and a name. This helps us organize the definition and remember all the parts. Also by having parallel conditions for addition and multiplication, we see how they are treated similarly. Second, you've probably seen all these conditions or some slight variations in an algebra course in the discussion of the properties of the real numbers, so the notation should be familiar. This is both a positive and a negative as you will be used to writing expressions with this notation and you use these properties

all the time, however, since we'll be using these properties to prove results, we need to be faithful to the conditions the way they are written and to not rely on our experience of how they should work. Third, it is important to look at what it says and what it doesn't say. For example, 0 and 1 are just names of certain objects in  $\mathbb{F}$  and don't have any other properties. No other elements are defined (does  $1 + 1 = 2$ ?) Also note that it doesn't define subtraction or division. Finally, although it is based on the real numbers there are many examples of fields, some of which are listed below:

### Examples:

1. Real numbers ( $\mathbb{R}$ ), with normal  $+$  and  $\cdot$ . This is the model for the axioms.
2. Rational numbers ( $\mathbb{Q}$ ), with normal  $+$  and  $\cdot$ .
3. Complex numbers ( $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ ) with normal  $+$  and  $\cdot$  ( $i^2 = -1$ ).
4.  $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$  with normal  $+$  and  $\cdot$ .
5.  $\{0, 1\}$  with addition and multiplication done *mod 2*. (*mod 2* means that you only look at the remainder when you divide by 2. For example  $1 + 1 = 0 \pmod{2}$ .)
6.  $\{0, 1, 2, \dots, p-1\} = \mathbb{Z}/p\mathbb{Z}$  where  $p$  is a prime, with addition and multiplication done *mod p*.
7.  $\{p(x)/q(x) : p, q \text{ polynomials}\}$  (rational functions) with the usual algebraic way of adding and multiplying such functions.

Examples are useful, but so are examples that don't quite fit the definitions.

### Near Examples: (these satisfy many, but not all of the axioms)

1. Integers ( $\mathbb{Z}$ ) with normal addition and multiplication.
2. The set of all  $n \times n$  matrices (for some fixed  $n$ ) with normal matrix addition and multiplication.
3. Quaternions ( $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$  where  $i, j, k$  are distinct and  $i^2 = j^2 = k^2 = ijk = -1$ ) with normal addition and multiplication otherwise.

Now for some important theorems:

**Theorem A:** For  $a, b \in \mathbb{F}$  there exists a unique  $x \in \mathbb{F}$  such that  $a + x = b$ .

**Proof:** Let  $a, b \in \mathbb{F}$ . Take  $x = -a + b$ . Since  $a \in \mathbb{F}$ ,  $-a \in \mathbb{F}$  (A5) and so  $-a + b \in \mathbb{F}$  (A1). Thus  $x \in \mathbb{F}$ . Also,  $a + (-a + b) = (a + -a) + b = 0 + b = b$  by (A3, A5, A4). So  $x$  satisfies  $a + x = b$ .

Now to show uniqueness, suppose there is a  $y \in \mathbb{F}$  with  $a + y = b$ . Then  $a + x = a + y$  since both equal  $b$ . Adding  $-a$  to both sides we get  $-a + (a + x) = -a + (a + y)$ . Simplifying using (A3, A5, A4), this reduces to  $x = y$ . Thus  $x = -a + b$  is the unique value in  $\mathbb{F}$  which satisfies  $a + x = b$ .

Two immediate consequences of Theorem A are that 0 is unique and for each  $a \in \mathbb{F}$ ,  $-a$  is unique.

The companion to Theorem A is Theorem M (for multiplication):

Theorem M: For  $a, b \in \mathbb{F}$  with  $a \neq 0$ , there exists a unique  $x \in \mathbb{F}$  such that  $a \cdot x = b$ .

Proof: Let  $a, b \in \mathbb{F}$  with  $a \neq 0$ . Take  $x = a^{-1} \cdot b$ . Since  $a \neq 0$ ,  $a^{-1}$  exists (M5) and so  $a^{-1} \cdot b \in \mathbb{F}$  (M1). Also  $a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b$  by (M3, M5, M4). So  $x \in \mathbb{F}$  and  $a \cdot x = b$ .

Now to show uniqueness, suppose there is a  $y \in \mathbb{F}$  with  $a \cdot y = b$ . Then  $a \cdot x = a \cdot y$  and by multiplying both sides by  $a^{-1}$  and simplifying, we get  $x = y$ . Thus  $x = a^{-1}b$  is the unique value in  $\mathbb{F}$  which satisfies  $a \cdot x = b$ .

Just like with Theorem A, we get from Theorem M immediately that 1 is unique and if  $a \in \mathbb{F}$  and  $a \neq 0$ , then  $a^{-1}$  is unique.

---

Now, we can expand on the idea of a field by again thinking about our model (the real numbers) and realizing that we have a way of comparing the size of two elements. Because we can compare, we can put the numbers in order, and so we have the following definition:

Definition: A field  $(\mathbb{F}, +, \cdot)$  is an **ordered field** if it satisfies the field axioms and there is a relation denoted by  $<$  satisfying the following 4 conditions (called the Order Axioms):

- O1: If  $a, b \in \mathbb{F}$  then one and only one of the following holds:  $a < b$ ,  $a = b$  or  $b < a$ . (Trichotomy)
- O2: For  $a, b, c \in \mathbb{F}$ , if  $a < b$  and  $b < c$  then  $a < c$ . (Transitive)
- O3: For  $a, b, c \in \mathbb{F}$ , if  $a < b$  then  $a + c < b + c$ . (Additive)
- O4: For  $a, b, c \in \mathbb{F}$ , if  $a < b$  and  $0 < c$  then  $a \cdot c < b \cdot c$ . (Multiplicative)

Now, if we go back to our examples of sets with operators that satisfy the field axioms, it is not so clear that all of them satisfy the order axioms.

The big question we want to address is what makes the real numbers so special? In other words, is there a property that they have that no other ordered field has? There is, but we'll get to that later. As a hint it has something to do with  $\sqrt{2}$ .