1 Fields

Reminder: If S is a set, then $x \in S$ means that x is an element of S.

1.1 Axioms

Suppose that $\mathbb{F}$ is a set, and that we have two operations on the set $\mathbb{F}$: $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ (called addition) and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ (called multiplication) so that the following statements are true:

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

A2. There exists a unique element $0 \in \mathbb{F}$ such that $a + 0 = 0 + a = a$ for every $a \in \mathbb{F}$.

A3. For all $a \in \mathbb{F}$, there exists a unique element $-a \in \mathbb{F}$ such that $a + (-a) = (-a) + a = 0$.

A4. For all $a, b \in \mathbb{F}$, $a + b = b + a$.

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

M2. There exists a unique element $1 \in \mathbb{F}$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in \mathbb{F}$.

M3. For all $a, b \in \mathbb{F}$, $a \cdot b = b \cdot a$.

M4. For all nonzero $a \in \mathbb{F}$, there exists a unique element $a^{-1} \in \mathbb{F}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

D1. For all $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

NT1. $1 \neq 0$.

Then $\mathbb{F}$ (with these two operations, and the special elements 0 and 1) is called a *field*.

A *ring* is a set with two operations, and special elements 0 and 1 which satisfies all of the above axioms except possibly (M4).

Notation 1. We will feel free to use the common notation ab to indicate $a \cdot b$. Although this does not usually cause confusion, we will sometimes need to be careful in our interpretation, i.e., "11" is not the same as "$1 \cdot 1$".

The basic example of a field is the set of real numbers, $\mathbb{R}$. Later, we will see (at least) two more examples: the set of rational numbers $\mathbb{Q}$, and the set $\mathbb{F}_p$, of equivalence classes of integers modulo p, where p is a prime number.

The integers form a ring, but not a field. We will later see that if m is a natural number then we can put operations on $\mathbb{Z}_m$ (the set of equivalence classes of integers modulo m) also form a ring. It will not be a field unless m is a prime.

2 Proving basic statements about fields using our axioms

Let $\mathbb{F}$ be a field.

Proposition 2. *For every $a \in \mathbb{F}$, $a0 = 0$.*

Proposition 3. *Let a and b be elements of $\mathbb{F}$. If $ab = 0$, then $a = 0$ or $b = 0$.*

Proposition 4. *0 has no multiplicative inverse. That is, there exists no $a \in \mathbb{F}$ such that $a0 = 1$.*

Proposition 5. *For all a, b, and c in $\mathbb{F}$, if $a + b = a + c$, then $b = c$.*

Proposition 6. *For all a, b, and c in $\mathbb{F}$, if $a \neq 0$ and $ab = ac$, then $b = c$.*

Proposition 7. *For every $a \in \mathbb{F}$, $-(-a) = a$.*

Proposition 8. *For every a and b in $\mathbb{F}$, $(-a)b = -(ab)$.*

Proposition 9. *For every a and b in $\mathbb{F}$, $(-a)(-b) = ab$.*