1.2 Fields and ordered fields

Of course the familiar number systems have additional structure. Besides the order, we have addition, subtraction, multiplication and division.

1.2.1 Definition. A *field* is a set $\mathbb{F}$ with two binary operations[2] $+$ and $\cdot$, called *addition* and *multiplication*, respectively, satisfying the following axioms:

(F1) (Associativity of addition) $(a+b)+c = a+(b+c)$ for all a, b, c in $\mathbb{F}$.

(F2) (Additive identity) There exists an element $0 \in \mathbb{F}$ such that $0 + a = a + 0 = a$ for all a.

(F3) (Additive inverses) For each a in $\mathbb{F}$ there exists an element $-a$ such that $(-a) + a = a + (-a) = 0$.

(F4) (Commutativity of addition) $a + b = b + a$ for all a, b in $\mathbb{F}$.

(F5) (Associativity of multiplication) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in $\mathbb{F}$.

(F6) (Multiplicative identity) There exists an element $1 \in \mathbb{F}$ such that $1 \cdot a = a \cdot 1 = a$ for all a.

(F7) (Multiplicative inverses) For all $a \neq 0$, there exists an element a^{-1} in $\mathbb{F}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(F8) (Commutativity of multiplication) $a \cdot b = b \cdot a$ for all a, b in $\mathbb{F}$.

(F9) (Distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c$.

(F10) (Nontriviality) $0 \neq 1$.

It is customary to omit the $\cdot$ when writing multiplication; in other words, we usually just write ab instead of $a \cdot b$. Additionally, we usually denote $a + (-b)$ simply by $a - b$, and we may also use the notation $\frac{1}{a}$ in place of a^{-1}. It is important to note that subtraction $-$ and division $\div$ are not really distinct operations; they are just syntactic shorthand for addition (resp. multiplication) by an additive (resp. multiplicative) inverse.

We also use the usual shorthand a^n in place of $\underbrace{a \cdots a}_{n \text{ times}}$ and na in place of $\underbrace{a + \cdots + a}_{n \text{ times}}$.

Remark. Though we shall be entirely concerned with fields in this course, you may be familiar with various mathematical objects satisfying fewer of the above axioms. A set with a single operation satisfying axioms (F1)–(F3) is a *group* which is said to be *commutative* or *abelian* if (F4) also holds.

A *ring* is a set with two operations satisfying all of the above except (F7), (F8) and (F10). A *commutative ring* satisfies (F8). According to some conventions, a ring need not satisfy (F6), though such "rings without identity" are sometimes cutely referred to as '*rng*'s. If (F7) holds but not (F8), then $\mathbb{F}$ is called a *division ring*.

Axiom (F10) might be considered optional for fields, but if we allow $0 = 1$ then $\mathbb{F}$ must be the one element set $\{0\}$ (you can prove this after you prove Proposition 1.2.4 below), which for various reasons is best not regarded as a field.

1.2.2 Example. Come up with some examples of fields, some with infinitely many and some with finitely many elements. Can you construct a field with exactly two elements? Three?

1.2.3 Proposition. *The following properties of addition and multiplication hold in any field. (That is, they follow from the axioms above.)*

(i) *(Uniqueness of identities) If an element b in $\mathbb{F}$ satisfies $b + a = a$ for some a, then $b = 0$. Likewise if b satisfies $ba = a$ for some $a \neq 0$, then $b = 1$.*

(ii) *(Uniqueness of inverses) If b satisfies $a + b = 0$, then $b = -a$. Likewise, if b satisfies $ba = 1$ then $b = a^{-1}$.*

(iii) *(Cancellation) If $a + c = b + c$ then $a = b$. Likewise if $c \neq 0$ and $ac = bc$, then $a = b$.*

(iv) *(Inverse of an inverse) $-(-a) = a$ and $(a^{-1})^{-1} = a$.*

[2] A binary operation is a function/operation taking in two elements of $\mathbb{F}$ and returning a third element of $\mathbb{F}$.

1.2.4 Proposition. *In any field, the following properties hold.*

(i) $0a = 0$ *for all* a.

(ii) *If* $ab = 0$, *then either* $a = 0$ *or* $b = 0$. *(We say* $\mathbb{F}$ *"has no divisors of zero".)*

(iii) $(-a)b = a(-b) = -(ab)$ *for all* a *and* b. *In particular* $-a = (-1)a$.

(iv) $(-a)(-b) = ab$ *for all* a *and* b.

1.2.5 Problem. In a field, show that if $b \neq 0$ and $d \neq 0$ then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

1.2.6 Definition. An *ordered field* is a field $\mathbb{F}$ equipped with a total order, so a set with a relation $\leq$ and two operations $+$ and $\cdot$ satisfying axioms (O1)–(O4) and (F1)–(F10), which is additionally required to satisfy the following axioms:

(OF1) (Compatibility of order and addition) If $a \leq b$ then $a + c \leq b + c$ for any c.

(OF2) (Compatibility of order and multiplication) If $a \leq b$ and $0 \leq c$, then $ac \leq bc$.

1.2.7 Example. Which examples from Example 1.2.2 are ordered fields? In case there is not an obvious order, is there any order at all satisfying (OF1) and (OF2)?

1.2.8 Proposition. *The following properties always hold in an ordered field.*

(a) *If* $0 \leq a$ *then* $-a \leq 0$.

(b) *If* $0 \leq a$ *and* $0 \leq b$ *then* $0 \leq ab$. *(In fact, this is equivalent to (OF2) and is often used in place of it as the other ordered field axiom).*

(c) *If* $a \leq 0$ *and* $0 \leq b$, *then* $ab \leq 0$.

(d) $0 \leq a^2$ *for any* a. *In particular* $0 < 1$.

(e) *If* $0 < a \leq b$ *then* $0 < b^{-1} \leq a^{-1}$.

In light of Proposition 1.2.4.(ii) *the above identities hold with strict inequality* $<$ *used in place of inequality* $\leq$.

1.2.9 Problem. Let $\mathbb{F}$ be an ordered field and consider the subset $Z \subset \mathbb{F}$ generated by taking 0, 1, $1+1$, $1+1+1$, etc. along with -1, $-1-1$, $-1-1-1$, etc. Show that this set is in bijection with the set of integers $\mathbb{Z}$.

Likewise, let $Q \subset \mathbb{F}$ be the subset generated by taking the multiplicative inverses of the nonzero elements in Z along with their integer multiples. Show that this set is in bijection with $\mathbb{Q}$.

Thus every ordered field contains a copy of $\mathbb{Q}$, which may be regarded as the "smallest" possible ordered field.