

Ordered Fields.

Definition 1. A **field** is an algebraic structure $\mathbb{F} = \langle F; +, -, 0, \cdot, 1 \rangle$ which satisfies the following

- (1) Additive laws¹:
 - (a) (Associative law) $\forall x \forall y \forall z ((x + (y + z)) = ((x + y) + z))$.
 - (b) (Commutative law) $\forall x \forall y (x + y = y + x)$.
 - (c) (Unit law) $\forall x (x + 0 = x)$
 - (d) (Inverse law) $\forall x (x + (-x) = 0)$
- (2) Multiplicative laws:
 - (a) (Associative law) $\forall x \forall y \forall z ((x(yz)) = ((xy)z))$.
 - (b) (Commutative law) $\forall x \forall y (xy = yx)$.
 - (c) (Unit law) $\forall x (x1 = x)$
- (3) Law linking addition to multiplication:
 - (a) (Distributive law): $\forall x \forall y \forall z (x(y + z) = xy + xz)$.
- (4) Other defining properties that are not laws:
 - (a) $0 \neq 1$.
 - (b) $\forall x ((x \neq 0) \rightarrow \exists y (xy = 1))$.

If you know the definition of “abelian group”, the axioms for fields say that \mathbb{F} is additively an abelian group, $\mathbb{F} - \{0\}$ is multiplicatively an abelian group, and the additive and multiplicative structures are linked by the distributive law.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ (p prime).

Nonexamples. $\mathbb{N}, \mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ (n not a prime).

Definition 2. An **ordered field** is a structure $\mathbb{F} = \langle F; +, -, 0, \cdot, 1, \leq \rangle$ where

- (1) $\langle F; +, -, 0, \cdot, 1 \rangle$ is a field,
- (2) $\langle F; \leq \rangle$ is a totally ordered set (which means that \leq is a reflexive, antisymmetric, transitive relation satisfying the trichotomy law),
- (3) (Order structure is linked to field structure):
 - (a) (Additive compatibility) $\forall x \forall y \forall z ((y \leq z) \rightarrow (x + y \leq x + z))$
 - (b) (Multiplicative compatibility) $\forall x \forall y \forall z (((y \leq z) \wedge (0 \leq x)) \rightarrow (xy \leq xz))$

If \mathbb{F} is an ordered field, then an element p is **positive** if $0 \leq p$ and $0 \neq p$ (we just abbreviate this with $0 < p$). The set P of all positive elements is called the **positive cone**. An element in $-P = \{-x \mid x \in P\}$ is called **negative**.

Examples. \mathbb{Q}, \mathbb{R} .

Nonexamples. $\mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ for any n .

¹A **law** or **identity** is a universally quantified equation.

Question: Why is impossible to order \mathbb{C} to make it an ordered field?

Thm. If \mathbb{F} is an order field with positive cone P , then the following are true.

- (1) (Can use $<$ in place of \leq)
 - (a) $\forall x \forall y \forall z ((y < z) \rightarrow (x + y < x + z))$
 - (b) $\forall x \forall y \forall z (((y < z) \wedge (0 < x)) \rightarrow (xy < xz))$
- (2) \mathbb{F} is the disjoint union $P \cup \{0\} \cup -P$.
- (3) The positive cone of \mathbb{F} is closed under addition and multiplication.
- (4) For any $a \in F - \{0\}$, a^2 is positive.

Proof.

I prove (1)(a) and leave (1)(b) as an exercise. Choose arbitrary field elements a, b, c and assume that $b < c$. We want to prove that $a + b < a + c$. Since $b < c$, we have $b \leq c$, so $a + b \leq a + c$ by (3)(a) of the definition of ordered fields. To show that $a + b < a + c$ holds we must rule out the possibility that $a + b = a + c$. For the purpose of obtaining a contradiction, assume that we do have $a + b = a + c$. Then using the field laws we deduce in order that

$$\begin{aligned}
 (-a) + (a + b) &= (-a) + (a + c) \\
 ((-a) + a) + b &= ((-a) + a) + c, \\
 ((a + (-a)) + b) &= ((a + (-a)) + c), \\
 (0 + b) &= (0 + c), \\
 (b + 0) &= (c + 0), \\
 b &= c,
 \end{aligned}$$

which is false. This contradiction shows that $\neg(a + b = a + c)$, so with our earlier conclusion (that $a + b \leq a + c$) we get $a + b < a + c$.

Item (2) follows from the law of trichotomy. (For every x , exactly one of the following is true: $0 < x$, $0 = x$, or $x < 0$. In the first case, $x \in P$; in the second, $x = \{0\}$; in the third, add $-x$ to both sides of $x < 0$ to obtain $0 < -x$, so $-x \in P$, so $x \in -P$.)

Item (3) follows from Item (1) by letting y be 0 and x be positive.

For Item (4), choose any $a \in F - \{0\}$. By Item (2), either $a \in P$ or $a \in -P$ (equivalently $-a \in P$). Therefore one of a^2 or the equal value $(-a)^2$ is the square of a positive element. By Item (3) we get $a^2 = (-a)^2 \in P$. \square

Cor. If \mathbb{F} is a field in which -1 is a sum of squares, then \mathbb{F} is not orderable.

Proof. Any nonzero sum of squares, such as $1 = 1^2$, belongs to P . Hence $-1 \in -P$. Since P contains all sums of squares, $-P$ contains -1 , and $P \cap -P = \emptyset$, we get that -1 cannot be a sum of squares. \square

Cor. The fields \mathbb{C} and $\mathbb{Z}/p\mathbb{Z}$ are not orderable.

Proof. In these fields, -1 is a sum of squares.

For \mathbb{C} , -1 is already a square.

For $\mathbb{Z}/p\mathbb{Z}$, 1 is a square, so $1 + 1 = 2$ is a sum of squares, and $1 + 1 + 1 = 3$ is a sum of squares, ETC. Thus every element of $\mathbb{Z}/p\mathbb{Z}$ is a sum of squares. \square