Fields

A field is a non-empty set $\mathbb{F}$ with two binary operations satisfying some properties. We usually call the elements of the set 'numbers', but the set could be a set of e.g. furniture. The binary operations we usually call 'addition' and 'multiplication' but they could be any well-defined binary operation. We also usually use $a + b$ and $a \cdot b$ to indicate these operations. In fact instead of $a \cdot b$ we often write ab. Now actually let's define a field:

Definition

A **Field** $\mathbb{F}$ is a non-empty set together with two binary operations, called addition ($+$) and multiplication ($\cdot$) such that

(a) For any $a, b \in \mathbb{F}$ we have $a + b \in \mathbb{F}$, and ($+$ is closed)

(b) For any $a, b \in \mathbb{F}$ we have $a \cdot b \in \mathbb{F}$ ($\cdot$ is closed)

and such that the following properties hold:

(1) For all $a, b \in \mathbb{F}$ we have $a + b = b + a$ ($+$ is commutative)

(2) For all $a, b, c \in \mathbb{F}$ we have $a + (b + c) = (a + b) + c$ ($+$ is associative)

(3) There exists a $0 \in \mathbb{F}$ such that for all $a \in \mathbb{F}$ we have $a + 0 = a$ (zero)

(4) For each $a \in \mathbb{F}$ there exists an element $-a \in \mathbb{F}$ such that $a + (-a) = 0$ (additive inverses/ opposites)

(5) For all $a, b \in \mathbb{F}$ we have $a \cdot b = b \cdot a$ ($\cdot$ is commutative)

(6) For all $a, b, c \in \mathbb{F}$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ($\cdot$ is associative)

(7) There exists a $1 \in \mathbb{F}$, $1 \neq 0$, such that $1 \cdot a = a$ for all $a \in \mathbb{F}$ (one, identity)

(8) For each $a \in \mathbb{F}$, $a \neq 0$, there exists an $a^{-1} \in \mathbb{F}$ such that $a \cdot a^{-1} = 1$ (multiplicative inverses/ reciprocals)

(9) For all $a, b, c \in \mathbb{F}$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributive property)

Example 1 **The Rational Numbers**

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \right\} \text{ with the usual } + \text{ and } \cdot$$

Example 2 **The Real Numbers**

$$\mathbb{R} \text{ with the usual } + \text{ and } \cdot$$

Example 3 **The Complex Numbers**

Let $\mathbb{C} = \{\, a + b\,\boldsymbol{i} \mid a, b \in \mathbb{R} \,\}$, and

(a) $(a + b\,\boldsymbol{i}) + (c + d\,\boldsymbol{i}) = (a + c) + (b + d)\,\boldsymbol{i}$

(b) $(a + b\,\boldsymbol{i}) \cdot (c + d\,\boldsymbol{i}) = (ac - bd) + (ad + bc)\,\boldsymbol{i}$

With these two operations $\mathbb{C}$ is a field.

We usually write:

- $0 + 0\,\boldsymbol{i} = 0$
- $1 + 0\,\boldsymbol{i} = 1$
- $a + 0\,\boldsymbol{i} = a$ [This way: $\mathbb{R} \subseteq \mathbb{C}$]
- $0 + 1\,\boldsymbol{i} = 0 + \boldsymbol{i} = \boldsymbol{i}$
- $0 + b\,\boldsymbol{i} = b\,\boldsymbol{i}$
- $a + 1\,\boldsymbol{i} = a + \boldsymbol{i}$
- $a + (-b)\,\boldsymbol{i} = a - b\,\boldsymbol{i}$

Note that

- $\boldsymbol{i}^2 = \boldsymbol{i} \cdot \boldsymbol{i} = (0 + \boldsymbol{i}) \cdot (0 + \boldsymbol{i}) = (0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 1 \cdot 0)\boldsymbol{i} = -1 + 0\,\boldsymbol{i} = -1$
- $-(a + b\,\boldsymbol{i}) = (-a) + (-b)\,\boldsymbol{i} = -a - b\,\boldsymbol{i}$
- $(a + b\,\boldsymbol{i})^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}\boldsymbol{i}$

Example 4 **The Field with 2 elements** (The smallest possible field)

Let $\mathbb{F}_2 = \{0, 1\}$ with the following addition and multiplication

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Example 5 **The Field with 4 elements**

Let $\mathbb{F}_4 = \{0, 1, a, b\}$ with the following

addition and multiplication

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Example 6 **The Field with 7 elements**

Let $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ with the following addition and multiplication

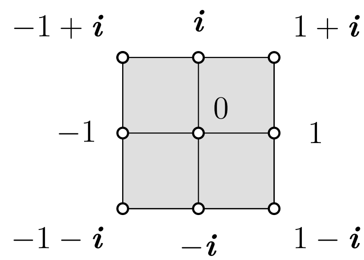
$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Note that these operation are just addition and multiplication modulo 7

Example 7 **The Field with 9 elements**

$$\mathbb{F}_9 \;=\; \{0,\; 1,\; 1+\boldsymbol{i},\; -\boldsymbol{i},\; -1-\boldsymbol{i},\; -1,\; -1-\boldsymbol{i},\; \boldsymbol{i},\; -1+\boldsymbol{i}\},$$



Multiplication and addition can be computed using the usual complex multiplication where the real and imaginary parts are 0 or $\pm 1 \pmod 3$:

$$(a+b\boldsymbol{i})+(c+d\boldsymbol{i}) = \underbrace{(a+c)}_{0,\pm 1 \pmod 3} + \underbrace{(c+d)}_{0,\pm 1 \pmod 3}\,\boldsymbol{i}$$

and

$$(a+b\boldsymbol{i})(c+d\boldsymbol{i}) = \underbrace{(ac-db)}_{0,\pm 1 \pmod 3} + \underbrace{(ad+bc)}_{0,\pm 1 \pmod 3}\,\boldsymbol{i}$$

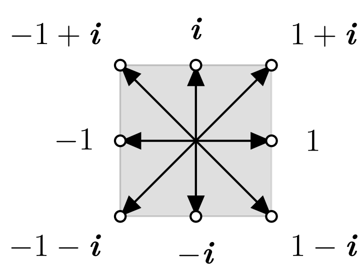
Example

$$(1+\boldsymbol{i})+(-1+\boldsymbol{i}) \;=\; 0+2\boldsymbol{i} \;=\; -\boldsymbol{i}$$

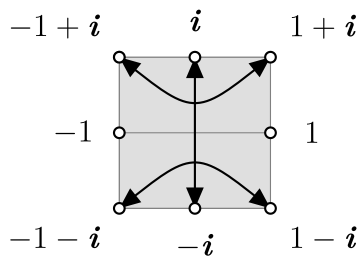
and

$$(1-\boldsymbol{i})(-1+\boldsymbol{i}) \;=\; 0+2\boldsymbol{i} \;=\; -\boldsymbol{i}$$

Note that the additive inverses are the usual opposites: $-z$



and the multiplicative inverses are:



$$(-1+\boldsymbol{i})(1+\boldsymbol{i})=1$$
$$1\cdot 1=1$$
$$(-\boldsymbol{i})\cdot\boldsymbol{i}=1$$
$$(-1)(-1)=1$$
$$(-1-\boldsymbol{i})(1-\boldsymbol{i})=1$$

Here are the complete tables of **addition**:

$+$	0	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$
0	0	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$
1	1	-1	$-1+\boldsymbol{i}$	$1-\boldsymbol{i}$	$-1-\boldsymbol{i}$	0	$-\boldsymbol{i}$	$1+\boldsymbol{i}$	$\boldsymbol{i}$
$1+\boldsymbol{i}$	$1+\boldsymbol{i}$	$-1+\boldsymbol{i}$	$-1-\boldsymbol{i}$	1	-1	$\boldsymbol{i}$	0	$1-\boldsymbol{i}$	$-\boldsymbol{i}$
$-\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	1	$\boldsymbol{i}$	$1+\boldsymbol{i}$	$-1-\boldsymbol{i}$	$-1+\boldsymbol{i}$	0	-1
$1-\boldsymbol{i}$	$1-\boldsymbol{i}$	$-1-\boldsymbol{i}$	-1	$1+\boldsymbol{i}$	$-1+\boldsymbol{i}$	$-\boldsymbol{i}$	$\boldsymbol{i}$	1	0
-1	-1	0	$\boldsymbol{i}$	$-1-\boldsymbol{i}$	$-\boldsymbol{i}$	1	$1-\boldsymbol{i}$	$-1+\boldsymbol{i}$	$1+\boldsymbol{i}$
$-1-\boldsymbol{i}$	$-1-\boldsymbol{i}$	$-\boldsymbol{i}$	0	$-1+\boldsymbol{i}$	$\boldsymbol{i}$	$1-\boldsymbol{i}$	$1+\boldsymbol{i}$	-1	1
$\boldsymbol{i}$	$\boldsymbol{i}$	$1+\boldsymbol{i}$	$1-\boldsymbol{i}$	0	1	$-1+\boldsymbol{i}$	-1	$-\boldsymbol{i}$	$-1-\boldsymbol{i}$
$-1+\boldsymbol{i}$	$-1+\boldsymbol{i}$	$\boldsymbol{i}$	$-\boldsymbol{i}$	-1	0	$1+\boldsymbol{i}$	1	$-1-\boldsymbol{i}$	$1-\boldsymbol{i}$

and **multiplication**:

$\cdot$	0	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$
0	0	0	0	0	0	0	0	0	0
1	0	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$
$1+\boldsymbol{i}$	0	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$	1
$-\boldsymbol{i}$	0	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$	1	$1+\boldsymbol{i}$
$1-\boldsymbol{i}$	0	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$
-1	0	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$
$-1-\boldsymbol{i}$	0	$-1-\boldsymbol{i}$	$\boldsymbol{i}$	$-1+\boldsymbol{i}$	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1
$\boldsymbol{i}$	0	$\boldsymbol{i}$	$-1+\boldsymbol{i}$	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$
$-1+\boldsymbol{i}$	0	$-1+\boldsymbol{i}$	1	$1+\boldsymbol{i}$	$-\boldsymbol{i}$	$1-\boldsymbol{i}$	-1	$-1-\boldsymbol{i}$	$\boldsymbol{i}$