Field

Definition: A *field* is a set $\mathbb{K}$ together with two *commutative* binary operations $+$ and $\cdot$, where $(\mathbb{K}, +)$ and $(\mathbb{K} \setminus 0, \cdot)$ are (Abelian) groups, and moreover $\forall a, b, c \in \mathbb{K} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

In other words the following axioms have to be satisfied:

- $\forall a, b \in \mathbb{K} : a + b = b + a$
- $\forall a, b, c \in \mathbb{K} : (a + b) + c = a + (b + c)$
- $\exists 0 \in \mathbb{K}\ \forall a \in \mathbb{K} : a + 0 = a$
- $\forall a \in \mathbb{K}\ \exists -a \in \mathbb{K} : a + (-a) = 0$
- $\forall a, b \in \mathbb{K} : a \cdot b = b \cdot a$ . . . including 0 !
- $\forall a, b, c \in \mathbb{K} \setminus 0 : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in \mathbb{K} \setminus 0\ \forall a \in \mathbb{K} \setminus 0 : a \cdot 1 = a$ . . . implies $1 \neq 0$
- $\forall a \in \mathbb{K} \setminus 0\ \exists a^{-1} \in \mathbb{K} \setminus 0 : a \cdot a^{-1} = 1$
- $\forall a, b, c \in \mathbb{K} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

The product symbol $\cdot$ is often omitted and it has priority to $+$.

Examples

$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$, briefly $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, are fields.

$\mathbb{Z}_p$ residue classes modulo a *prime* p are fields ($\mathbb{Z}_4$ and $\mathbb{Z}_6$ are not!)

$\mathbb{Z}_7$:

$+$	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

These binary operations $+$ and $\cdot$ satisfy all axioms.

In particular, the negative and inverse elements are:

x	0	1	2	3	4	5	6
$-x$	0	6	5	4	3	2	1

x	0	1	2	3	4	5	6
x^{-1}		1	4	5	2	3	6

The set $\left\{ \frac{p(x)}{q(x)} \right\}$ with p, q polynomials with real coefficients forms the field $\mathbb{R}(x)$ of *real rational functions*.

Metatheorem

Metatheorem: All statements about systems of equations and matrices over $\mathbb{R}$ are valid also for any field $\mathbb{K}$.
. . . in the proofs were only used properties specified in field axioms.

Example: A solution of a system $\boldsymbol{Ax} = \boldsymbol{b}$ over $\mathbb{Z}_7$:
1. We transform the augmented matrix into the echelon form:

$$(\boldsymbol{A}|\boldsymbol{b}) = \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 3 & 1 & 2 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 2 & 4 & 1 & 4 \end{array}\right)$$

$$\sim \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

2. If the last column contains a pivot, the system has no solution.

3. Otherwise we first describe all solutions of the homogeneous system $\boldsymbol{A}\bar{\boldsymbol{x}} = \boldsymbol{0}$, i.e.

$$\begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix} \bar{\boldsymbol{x}} = \boldsymbol{0}$$

$$\begin{aligned} \bar{x}_2 &= -4\bar{x}_4 - 2\bar{x}_3 = 3\bar{x}_4 + 5\bar{x}_3 \\ \bar{x}_1 &= -4\bar{x}_3 - 2\bar{x}_2 = 3\bar{x}_3 + 5(3\bar{x}_4 + 5\bar{x}_3) = \bar{x}_4 \end{aligned}$$

By using parameters p_1 and p_2:

$$\begin{aligned} \bar{x}_1 &= p_2 \\ \bar{x}_2 &= 5p_1 + 3p_2 \\ \bar{x}_3 &= p_1 \\ \bar{x}_4 &= p_2 \end{aligned} \quad \text{i.e. } \bar{\boldsymbol{x}} = \begin{pmatrix} 0 \\ 5 \\ 1 \\ 0 \end{pmatrix} p_1 + \begin{pmatrix} 1 \\ 3 \\ 0 \\ 1 \end{pmatrix} p_2$$

4. Finally, by the backward substitution we find any solution of $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$, e.g. $\boldsymbol{x}^0 = (4, 2, 0, 0)^T$ and get:

$$\boldsymbol{x} = (4, 2, 0, 0)^T + p_1(0, 5, 1, 0)^T + p_2(1, 3, 0, 1)^T$$

Metatheorem

Example: A matrix inversion over $\mathbb{Z}_5$:

$$(\boldsymbol{A}|\boldsymbol{I}_n) = \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 4 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 4 & 4 & 2 \\ 0 & 1 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 3 & 4 & 0 \end{array}\right) = (\boldsymbol{I}_n|\boldsymbol{A}^{-1})$$

Test:

			4	4	2
			2	1	1
			3	4	0
1	3	2	1	0	0
3	4	0	0	1	0
0	1	1	0	0	1

Field properties

Observations: In any field $\forall a : 0a = 0, (-1)a = -a$,

Proof:

$$0a = 0a + 0 = 0a + (0a - 0a) = (0 + 0)a - 0a = 0a - 0a = 0$$

$$\begin{aligned}(-1)a &= (-1)a + 0 = (-1)a + a - a = (-1)a + 1a - a \\ &= (-1 + 1)a - a = 0a - a = 0 - a = -a\end{aligned}$$

Observation: If $ab = 0$ then $a = 0$ or $b = 0$.

Proof: By contradiction, if $a, b \neq 0$ then $\exists a^{-1}, b^{-1}$.
Then $1 = aa^{-1}bb^{-1} = aba^{-1}b^{-1} = 0a^{-1}b^{-1} = 0$ a contradiction.

Fields from modular arithmetic

Theorem: $\mathbb{Z}_p$ is a field if and only if p is a prime.

Proof: $\Rightarrow$: If $p = ab$ was composed then $ab \equiv 0 \pmod{p}$, a contradiction with the observation.

$\Leftarrow$: most of the axioms follow from the properties of $+$ and $\cdot$ on $\mathbb{Z}$. The only different is the existence of the inverse element a^{-1}: $\forall a \in \{1, \ldots, p-1\}\ \exists a^{-1} \in \{1, \ldots, p-1\} : aa^{-1} \equiv 1 \pmod{p}$.

Define $f_a : \{1, \ldots, p-1\} \to \{1, \ldots, p-1\}$ by $f_a(x) = ax \mod p$. Since f_a is from a finite set to itself, then *if f_a is injective* then f_a is surjective and exists b such that $f_a(b) = 1$, i.e. $ab \equiv 1 \pmod{p}$.

If f_a was not injective then $\exists b, c$ w.l.o.g. $b > c$ s.t. $f_a(b) = f_a(c) \Rightarrow 0 = f_a(b) - f_a(c) \equiv ab - ac = a(b-c) \pmod{p}$, in contrary with p being a prime as $a, b - c \in \{1, \ldots, p-1\}$.

Galois fields

Theorem: A field of size n exists if and only if n is a power of prime. It is unique upto isomorphism. We denote it by $GF(n)$.

Example: The field $GF(4) = GF(2^2)$: For $T = \{0, 1, a, b\}$ define the addition and multiplication as:

$+$	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

These operations $+$ and $\cdot$ satisfy all axioms.

Another view on the same field: take T as all polynomials of the maximum degree 1 with coefficients in $\mathbb{Z}_2$, e.g. $a = x$, $b = x + 1$. The multiplication is done modulo the polynomial $x^2 + x + 1$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Characteristic

Definition: For a field $\mathbb{K}$, if for some $n \in \mathbb{N}$: $\underbrace{1+1+\cdots+1}_{n\times} = 0$

then the smallest such n is the *characteristic* of the field $\mathbb{K}$.
Otherwise the field $\mathbb{K}$ has characteristic 0.

Theorem: The field characteristic is always a prime or 0.

Proof: By contrary, if the characteristic was composed $n = ab$, then
$0 = \underbrace{1+1+\cdots+1}_{n\times} = \underbrace{(1+1+\cdots+1)}_{a\times}\underbrace{(1+1+\cdots+1)}_{b\times} \neq 0$
as both $\underbrace{1+1+\cdots+1}_{a\times} \neq 0$ and $\underbrace{1+1+\cdots+1}_{b\times} \neq 0$.

Observation: In fields of characteristic 2 each element is self-inverse and subtraction can be replaced by addition.
Proof: $1+1=0 \;\Rightarrow\; -1=1 \;\Rightarrow\; -a=a \;\Rightarrow\; a-b=a+b$.

Fermat's little theorem

Theorem: [Fermat 1640•, Leibnitz 1683+, Euler 1736*]
For any prime p and any $a \in \{1, \ldots, p-1\}$: $a^{p-1} \equiv 1 \pmod{p}$.

Proof:
In $\mathbb{Z}_p$ the map $f_a : i \to ai$
is bijective on $\{1, \ldots, p-1\}$, hence

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} ai = a^{p-1} \prod_{i=1}^{p-1} i$$

Corollary: In $\mathbb{Z}_p$ with p prime
any a satisfies $a^p = a$.

Pierre de Fermat
1607 – 1665

•w/o proof, +unpublished, *published