Fields

Table of contents

The definition 1
Examples and non-examples 2
$\mathbb{Z}_n$ is a field exactly when n is prime 3
Calculating in a field 5
Solving linear equations 6
Common mistakes 8
See also 9

A field is a set with two operations, $+$ and $\cdot$, in which you can add, subtract, multiply, and divide by anything except 0, with all the usual rules holding. Formally it is two abelian groups[1] on one set, $(F,+)$ on all of it and $(F-\{0\},\cdot)$ on everything but 0, tied together by the distributive laws. $\mathbb{Q}$ and $\mathbb{R}$ are fields, $\mathbb{Z}$ is not, and $\mathbb{Z}_n$ (integers-modulo-n[2]) is a field exactly when n is prime. In a field every linear equation $ax+b=c$ with $a\neq 0$ has exactly one solution. First met in 2026-10-08-definitions-and-examples-of-fields[3].

The definition

Definition. A **field** $(F,+,\cdot)$ is a set F with two binary operations $+$ and $\cdot$ such that

(1) $(F,+)$ is an abelian group;

(2) $(F-\{0\},\cdot)$ is an abelian group, where 0 is the identity of $(F,+)$; and

(3) for all $f,g,h\in F$, $f\cdot(g+h)=(f\cdot g)+(f\cdot h)$ and $(f+g)\cdot h=(f\cdot h)+(g\cdot h)$.

[1] courses/math1061/groups.pdf
[2] courses/math1061/integers-modulo-n.pdf
[3] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

Written out, conditions (1) and (2) are five checks each, side by side:

	Addition, on F	Multiplication, on $F - \{0\}$
closure	$f + g \in F$	$f, g \neq 0 \Rightarrow f \cdot g \neq 0$
associativity	$(f + g) + h = f + (g + h)$	$(f \cdot g) \cdot h = f \cdot (g \cdot h)$
identity	0, with $0 + f = f + 0 = f$	1, with $1 \cdot f = f \cdot 1 = f$
inverses	every f has $-f$, with $f + (-f) = 0$	every $f \neq 0$ has f^{-1}, with $f \cdot f^{-1} = 1$
commutativity	$f + g = g + f$	$f \cdot g = g \cdot f$

Condition (3) is the two distributive laws, which hold for all $f, g, h \in F$, zero included.

Points that are easy to read past:

- **The two identities are named 0 and 1 by their jobs,** not because they are the integers 0 and 1. In $\mathbb{Z}_n$ they are [0] and [1]. The "0" removed in condition (2) is whatever the additive identity is.
- **Closure in (2) is a real condition.** It says that a product of two non-zero elements is never 0. It is the condition $\mathbb{Z}_4$ and $\mathbb{Z}_{15}$ fail.
- **$-f$ and f^{-1} are different inverses.** Each element has an additive inverse, and each non-zero element has a multiplicative one as well. In $\mathbb{Z}_5$, $-[2] = [3]$ and $[2]^{-1} = [3]$ happen to agree, but $-[4] = [1]$ while $[4]^{-1} = [4]$.
- **The distributive laws are the only link between the operations.** Without (3), a field would be two unrelated groups that happen to share a set.

Why 0 is left out of (2). In any field, $0 \cdot f = 0$ for every f. By the distributive law,

$$0 \cdot f = (0 + 0) \cdot f = (0 \cdot f) + (0 \cdot f),$$

and adding $-(0 \cdot f)$ to both sides leaves $0 = 0 \cdot f$. So $0 \cdot y = 1$ has no solution, and 0 can never have a multiplicative inverse. Asking for a group on all of F under $\cdot$ would rule out every field, just as 0 stops $(\mathbb{R}, \cdot)$ being a group (groups[4]).

Examples and non-examples

	Field?	Why
$(\mathbb{Q}, +, \cdot)$	**yes**	every non-zero $\frac{a}{b}$ has inverse $\frac{b}{a}$
$(\mathbb{R}, +, \cdot)$	**yes**	every non-zero x has inverse $\frac{1}{x}$

[4] courses/math1061/groups.pdf

	Field?	Why
$(\mathbb{Z}, +, \cdot)$	**no**	2 has no multiplicative inverse in $\mathbb{Z}$
$(\mathbb{Z}_7, +, \cdot)$	**yes**	7 is prime
$(\mathbb{Z}_4, +, \cdot)$	**no**	$[2] \cdot [2] = [0]$: closure fails in (2)
$(\mathbb{Z}_{15}, +, \cdot)$	**no**	$[3] \cdot [5] = [0]$: closure fails in (2)
$(\mathbb{Z}_{12}, +, \cdot)$	**no**	$[2]$ has no inverse, since $2k$ is even and never $\equiv 1 \pmod{12}$

$\mathbb{Z}$, $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{15}$ are worked in 2026-10-08-definitions-and-examples-of-fields[5] and 2026-10-08-definitions-and-examples-of-fields[6]. $\mathbb{Z}_{12}$ is Q2 of practice-problems[7], and Q3 of the same set checks every condition for an unfamiliar field on $\mathbb{Q} \times \mathbb{Q}$.

Every one of the non-examples passes (1) and (3) and fails (2). That is the usual pattern: addition is rarely the problem, and the work in deciding whether something is a field is in the multiplicative group.

To show something is not a field, one failure with specific elements is enough, as for groups: "2 has no inverse in $\mathbb{Z}$", or "$[3] \cdot [5] = [0]$ in $\mathbb{Z}_{15}$".

$\mathbb{Z}_n$ is a field exactly when n is prime

$(\mathbb{Z}_n, +)$ is a group for every $n \in \mathbb{Z}^+$.
$(\mathbb{Z}_p, +, \cdot)$ is a field when p is prime.

For any n, condition (1) holds (integers-modulo-n[8]), and condition (3), associativity, commutativity and the identity $[1]$ for multiplication are all inherited from the integers, for example $[a]([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$. So whether $\mathbb{Z}_n$ is a field comes down to two things about $\mathbb{Z}_n - \{[0]\}$: is it **closed** under multiplication, and does every class in it have an **inverse**?

When n is composite, closure fails. Write $n = rs$ with $1 < r, s < n$. Then $[r]$ and $[s]$ are non-zero, but

$$[r] \cdot [s] = [rs] = [n] = [0].$$

$\mathbb{Z}_4$ $(2 \cdot 2)$, $\mathbb{Z}_6$ $(2 \cdot 3)$, $\mathbb{Z}_{12}$ $(3 \cdot 4)$ and $\mathbb{Z}_{15}$ $(3 \cdot 5)$ all fail this way. A non-zero class that multiplies something non-zero into $[0]$ also has no inverse: if $[a][b] = [0]$ with $[b] \neq [0]$, multiplying both

[5] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[6] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[7] courses/math1061/practice-problems.pdf
[8] courses/math1061/integers-modulo-n.pdf

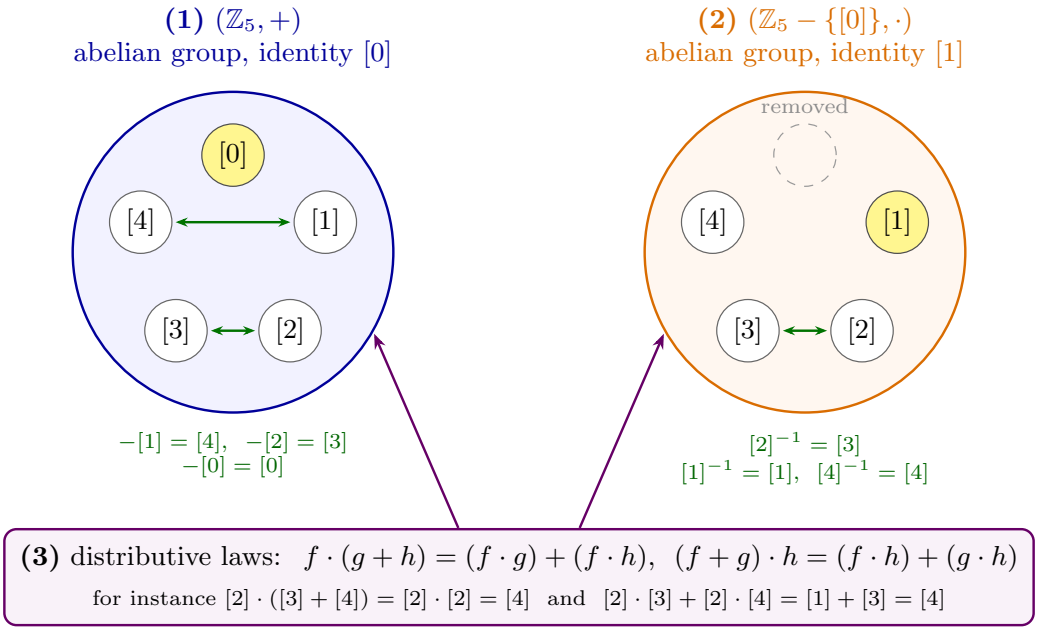


Figure 1: A field is two abelian groups on one set, shown for $\mathbb{Z}_5$. Left: all five classes under addition, identity [0]. A line joins each class to its additive inverse; [0] is its own. Right: the same classes under multiplication, with [0] taken out and identity [1]. [2] and [3] are inverses, and [1] and [4] are their own. The same class can have different inverses in the two groups: $-[4] = [1]$ but $[4]^{-1} = [4]$. Below: the distributive laws, the one condition that mentions both operations, checked on one instance.

sides by an inverse of $[a]$ would give $[b] = [0]$. That is why $[2]$, with $[2][6] = [0]$, has no inverse in $\mathbb{Z}_{12}$.

When $n = p$ is prime, both hold.

- *Closure.* If $[a] \cdot [b] = [0]$ then $p \mid ab$. The prime p appears in the prime factorisation of ab, which is the factorisation of a together with that of b (divisibility-and-factorisation[9]), so $p \mid a$ or $p \mid b$. That is, $[a] = [0]$ or $[b] = [0]$. A product of non-zero classes is non-zero.
- *Inverses.* Fix $[a] \neq [0]$ and look at its row of the table, $[a][1], [a][2], \ldots, [a][p-1]$. By closure none of these is $[0]$. No two are equal: if $[a][b] = [a][c]$ then $p \mid a(b-c)$, and since $p \nmid a$, the same argument gives $p \mid (b-c)$, so $[b] = [c]$. That is $p-1$ different non-zero classes, which is all of them, so one of them is $[1]$. Whichever $[b]$ gives it is $[a]^{-1}$.

So $\mathbb{Z}_n$ is a field for $n = 2, 3, 5, 7, 11, 13, \ldots$ and for no other $n \geq 2$. ($\mathbb{Z}_1$ has one class, $\mathbb{Z}_1 - \{[0]\}$ is empty, and the empty set has no identity, so it is not a field either.)

$\mathbb{Z}_5 - \{[0]\}$: closed, every row has $[1]$

$\cdot$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	(1)	$[2]$	$[3]$	$[4]$
$[2]$	$[2]$	$[4]$	(1)	$[3]$
$[3]$	$[3]$	(1)	$[4]$	$[2]$
$[4]$	$[4]$	$[3]$	$[2]$	(1)

$\mathbb{Z}_6 - \{[0]\}$: not closed

$\cdot$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	
$[1]$	(1)	$[2]$	$[3]$	$[4]$	$[5]$	
$[2]$	$[2]$	$[4]$	**[0]**	$[2]$	$[4]$	no [1]
$[3]$	$[3]$	**[0]**	$[3]$	**[0]**	$[3]$	no [1]
$[4]$	$[4]$	$[2]$	**[0]**	$[4]$	$[2]$	no [1]
$[5]$	$[5]$	$[4]$	$[3]$	$[2]$	(1)	

Figure 2: Multiplication on the non-zero classes of $\mathbb{Z}_5$ and of $\mathbb{Z}_6$. Left, $p = 5$ prime: no product is $[0]$, so the set is closed, and $[1]$ (ringed) appears once in every row and every column, so every class has an inverse. Right, $n = 6 = 2 \cdot 3$: the red cells are products of two non-zero classes that come out as $[0]$, so closure fails. The rows of $[2]$, $[3]$ and $[4]$, the classes sharing a factor with 6, contain no $[1]$, so those classes have no inverse. Only $[1]$ and $[5]$ do.

Calculating in a field

The two inverses give the other two operations:

[9] courses/math1061/divisibility-and-factorisation.pdf

- **Subtraction** is adding the additive inverse: $f - g = f + (-g)$.
- **Division** is multiplying by the multiplicative inverse: $f \div g = f \cdot g^{-1}$, for $g \neq 0$.

In $\mathbb{Q}$ and $\mathbb{R}$ these are the familiar operations. In $\mathbb{Z}_p$:

- $-[a] = [-a] = [p - a]$. In $\mathbb{Z}_{11}$, $-[3] = [8]$, because $[3] + [8] = [11] = [0]$.
- $[a]^{-1}$ is the class $[b]$ with $ab \equiv 1 \pmod{p}$. It is never a fraction: in $\mathbb{Z}_{11}$, $[2]^{-1} = [6]$, because $2 \cdot 6 = 12 \equiv 1$. Ways to find it are in integers-modulo-n[10].

So "$5 \div 2$" in $\mathbb{Z}_{11}$ is $[5] \cdot [6] = [30] = [8]$, and indeed $[2] \cdot [8] = [16] = [5]$.

Solving linear equations

To solve $ax + b = c$ in a field, with $a \neq 0$:

1. **Add $-b$ to both sides**, which exists by (1): $ax = c + (-b)$.
2. **Multiply both sides by a^{-1}**, which exists by (2) because $a \neq 0$: $x = a^{-1} \cdot (c + (-b))$.
3. **Check** by substituting back.

Each step is reversible, since b and a can be put back by adding b and multiplying by a. So the equation has **exactly one solution**, $x = a^{-1}(c - b)$. It is the two-group version of solving $a * x = b$ in a group (groups[11]).

Worked: an equation in $\mathbb{Z}_{13}$

Solve $5x + 7 = 3$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.

$$\begin{aligned} 5x + 7 &= 3 && \\ 5x &= 3 + (-7) = -4 = 9 && \text{add } -7 \\ 8 \cdot 5x &= 8 \cdot 9 && [5]^{-1} = [8], \text{ since } 5 \cdot 8 = 40 = 3 \cdot 13 + 1 \\ x &= 72 = 7 && 72 = 5 \cdot 13 + 7 \end{aligned}$$

Check: $5 \cdot 7 + 7 = 42 = 3 \cdot 13 + 3 \equiv 3 \pmod{13}$. ✓ So $x = [7]$.

With a bracket, multiply by the inverse first. For $3(x + 2) = 5$ in $\mathbb{Z}_7$: $[3]^{-1} = [5]$, so $x + 2 = 5 \cdot 5 = 25 = 4$, and $x = 4 - 2 = [2]$. *Check:* $3(2 + 2) = 12 \equiv 5 \pmod{7}$. Expanding with the distributive law first, $3x + 6 = 5$, gives the same answer by the usual two steps.

[10] courses/math1061/integers-modulo-n.pdf
[11] courses/math1061/groups.pdf

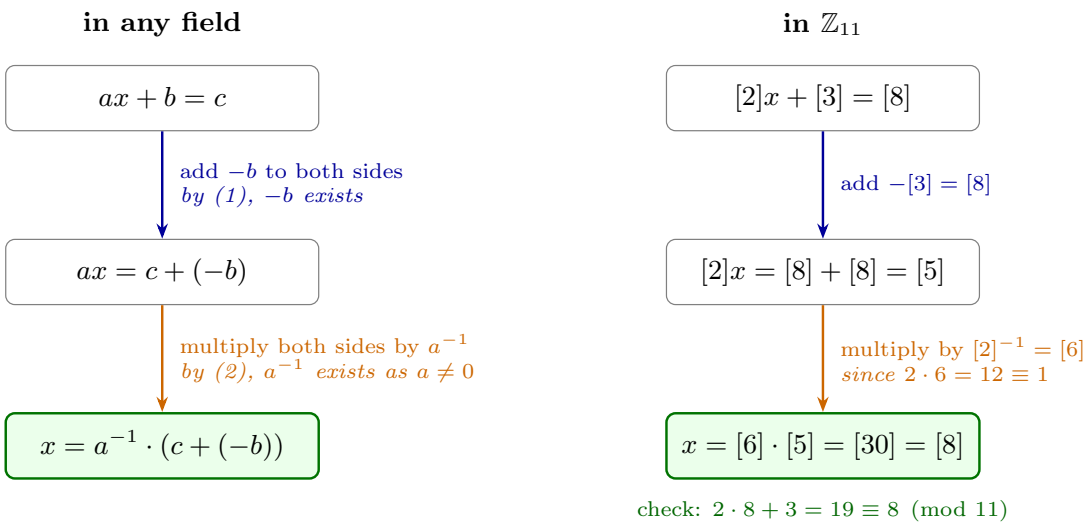


Figure 3: Solving $ax + b = c$ in a field, on the left in general and on the right for $2x + 3 = 8$ in $\mathbb{Z}_{11}$. Each arrow applies one inverse to both sides. The first uses the additive group, condition (1): every element, here [3], has a negative, $[-3] = [8]$. The second uses the multiplicative group, condition (2): every non-zero element, here [2], has an inverse, [6]. Neither step can fail in a field, so the equation always has exactly one solution.

The two equations of 2026-10-08-definitions-and-examples-of-fields[12] are worked the same way: $2x + 3 = 8$ in $\mathbb{Z}_{11}$ gives $x = [8]$, and $10x + 9 = 6$ in $\mathbb{Z}_{17}$ gives $x = [15]$. More are in practice-problems[13], Q1.

From a class to an integer

A solution in $\mathbb{Z}_p$ is a class, and the integers y satisfying the matching congruence are exactly the members of that class. For $2y + 3 \equiv 8 \pmod{11}$ they are $[8] = \{\dots, -3, 8, 19, \dots\}$. The **smallest positive** one is the usual representative of the class when that is between 1 and $p - 1$, and p itself when the solution is $[0]$. In the column picture of integers-modulo-n[14] it is the shaded entry of the column, or the entry just below it for $[0]$. A negative representative, such as -2 for $[15]$ in $\mathbb{Z}_{17}$, names the right class but is not the positive integer asked for.

When the set is not a field

In $\mathbb{Z}_{15}$, $[3]$ has no inverse, and the method breaks in both possible ways:

- $3x = 5$ has **no** solution, because $3x$ is always one of $[0], [3], [6], [9], [12]$;
- $3x = 6$ has **three**, $x = [2], [7], [12]$.

Exactly one solution for every $a \neq 0$ is what being a field buys.

Common mistakes

- **Checking only addition.** $(F, +)$ is usually the easy part. The work is in $(F - \{0\}, \cdot)$, and that is where $\mathbb{Z}$, $\mathbb{Z}_4$ and $\mathbb{Z}_{15}$ fail.
- **Asking 0 for a multiplicative inverse,** or forgetting to remove it. Condition (2) is about $F - \{0\}$.
- **Assuming every $\mathbb{Z}_n$ is a field.** Only prime n works. For composite n, removing $[0]$ is not enough, because other products land on $[0]$.
- **Leaving a fraction in $\mathbb{Z}_p$.** $2x = 5$ in $\mathbb{Z}_{11}$ does not give $x = \frac{5}{2}$. It gives $x = [6][5] = [8]$.
- **Using the wrong inverse.** To clear "$+3$" add $-[3]$; to clear "$2\cdot$" multiply by $[2]^{-1}$. In $\mathbb{Z}_{11}$ these are $[8]$ and $[6]$, different classes.
- **Not reducing the answer.** $x = [-36]$ in $\mathbb{Z}_{17}$ is correct but unfinished: it is $[15]$. If a question wants the smallest positive integer, a negative representative is not it.
- **Skipping the check.** Substituting back takes one line and catches an inverse found wrongly.

[12] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[13] courses/math1061/practice-problems.pdf
[14] courses/math1061/integers-modulo-n.pdf

- **Forgetting the distributive laws** when checking an unfamiliar structure. They are a separate condition, and two groups on one set without them are not a field.

See also

- groups[15] — the four properties behind conditions (1) and (2), and solving $a * x = b$
- integers-modulo-n[16] — $\mathbb{Z}_n$, $\mathbb{Z}_p$, and finding multiplicative inverses mod p
- subgroups-and-cyclic-groups[17] — subgroups, $\langle a \rangle$, and cyclic groups
- divisibility-and-factorisation[18] — unique factorisation, used for why $\mathbb{Z}_p$ is a field
- cayley-tables[19] — reading closure and inverses off a table
- 2026-10-08-definitions-and-examples-of-fields[20] — Lecture 28
- practice-problems[21] — §36, with full worked solutions

[15] courses/math1061/groups.pdf
[16] courses/math1061/integers-modulo-n.pdf
[17] courses/math1061/subgroups-and-cyclic-groups.pdf
[18] courses/math1061/divisibility-and-factorisation.pdf
[19] courses/math1061/cayley-tables.pdf
[20] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[21] courses/math1061/practice-problems.pdf