Lecture 28 — Definitions and Examples of Fields

Table of contents

Goals . . . 1
Cyclic subgroups . . . 2
Cyclic groups . . . 3
The definition of a field . . . 5
Fields already in use . . . 6
Worked: is $(\mathbb{Z}_4, +, \cdot)$ a field? . . . 6
Worked: which of these is a field? . . . 7
Solving equations in a field . . . 8
See also . . . 10

The cyclic subgroups of $\mathbb{Z}_8$ and which groups are cyclic, then fields: a set with two operations that is an abelian group under each of them, joined by the distributive laws. Which of $\mathbb{Z}$, $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{15}$ are fields, and how to solve a linear equation in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{17}$. Pre-work: Video 036 (Definitions and Examples of Fields). Fields are collected in fields[1], cyclic subgroups and cyclic groups in subgroups-and-cyclic-groups[2], and $\mathbb{Z}_p$ and multiplicative inverses mod p in integers-modulo-n[3]. The group definition everything here leans on is in groups[4].

Goals

1. Review the concepts of **groups**, **abelian groups**, **subgroups** and **cyclic subgroups**.
2. Become familiar with calculations in **fields**.
3. Learn how to solve equations in fields.

The four terms in the first goal, in one line each:

[1] courses/math1061/fields.pdf
[2] courses/math1061/subgroups-and-cyclic-groups.pdf
[3] courses/math1061/integers-modulo-n.pdf
[4] courses/math1061/groups.pdf

- **Group.** A set with a binary operation, $(G, *)$, satisfying closure, associativity, identity and inverses (groups[5]).
- **Abelian.** $a * b = b * a$ for all $a, b \in G$.
- **Subgroup.** A subset of G that is a group under the same operation (subgroups-and-cyclic-groups[6]).
- **Cyclic subgroup.** $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, every power of a: positive, zero and negative.

Cyclic subgroups

If $(G, *)$ is a group and $a \in G$, then

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

is a subgroup of G, and is called the **cyclic subgroup of G generated by a.**

The powers are taken with the group's own operation: $a^2 = a * a$, $a^0 = e$, and $a^{-i} = (a^{-1})^i$. In an additive group such as $(\mathbb{Z}_n, +)$ a "power" is a repeated sum, so $[a]^i = [ia]$, and $\langle [a] \rangle$ is the set of multiples of $[a]$. The full treatment is in subgroups-and-cyclic-groups[7].

Worked: the cyclic subgroups of $(\mathbb{Z}_8, +)$

Determine all the cyclic subgroups of $(\mathbb{Z}_8, +)$.

$\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$, so there are eight elements to try. For each, keep adding $[a]$ until the sum comes back to $[0]$; after that the list repeats. The negative powers add nothing new: if k copies of $[a]$ make $[0]$, then $[a]^{-1} = [a]^{k-1}$, so every negative power is already one of the positive ones.

$$\begin{aligned}
\langle [0] \rangle &= \{[0]\} \\
\langle [1] \rangle &= \{[1], [2], [3], [4], [5], [6], [7], [8] = [0]\} = \mathbb{Z}_8 \\
\langle [2] \rangle &= \{[2], [4], [6], [8] = [0]\} = \{[0], [2], [4], [6]\} \\
\langle [3] \rangle &= \{[3], [6], [9] = [1], [4], [7], [10] = [2], [5], [8] = [0]\} = \mathbb{Z}_8 \\
\langle [4] \rangle &= \{[4], [8] = [0]\} = \{[0], [4]\}
\end{aligned}$$

The other three, $\langle [5] \rangle$, $\langle [6] \rangle$ and $\langle [7] \rangle$, need no new work, because of two rules that hold in any group:

- $\langle e \rangle = \{e\}$**.** Every power of the identity is the identity. That is $\langle [0] \rangle = \{[0]\}$ above.

[5] courses/math1061/groups.pdf
[6] courses/math1061/subgroups-and-cyclic-groups.pdf
[7] courses/math1061/subgroups-and-cyclic-groups.pdf

- $\langle a \rangle = \langle a^{-1} \rangle$**.** The powers of a^{-1} are $(a^{-1})^i = a^{-i}$, and as i runs through $\mathbb{Z}$ so does $-i$. The two lists are the same powers taken in the opposite order.

In $(\mathbb{Z}_8, +)$ the inverse of $[a]$ is $[-a] = [8-a]$, so $[5] = [3]^{-1}$, $[6] = [2]^{-1}$ and $[7] = [1]^{-1}$:

$$\langle [5] \rangle = \langle [3] \rangle = \mathbb{Z}_8, \qquad \langle [6] \rangle = \langle [2] \rangle = \{[0], [2], [4], [6]\}, \qquad \langle [7] \rangle = \langle [1] \rangle = \mathbb{Z}_8.$$

So $\mathbb{Z}_8$ has four distinct cyclic subgroups, $\{[0]\}$, $\{[0], [4]\}$, $\{[0], [2], [4], [6]\}$ and $\mathbb{Z}_8$ itself, and

$$\langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle = \mathbb{Z}_8.$$

The four elements that reach everything are the odd ones. An even step from [0] only ever lands on even classes. The four subgroups sit inside one another, $\{[0]\} \subseteq \{[0], [4]\} \subseteq \{[0], [2], [4], [6]\} \subseteq \mathbb{Z}_8$, as drawn in 2026-10-06-elementary-properties-of-groups[8].

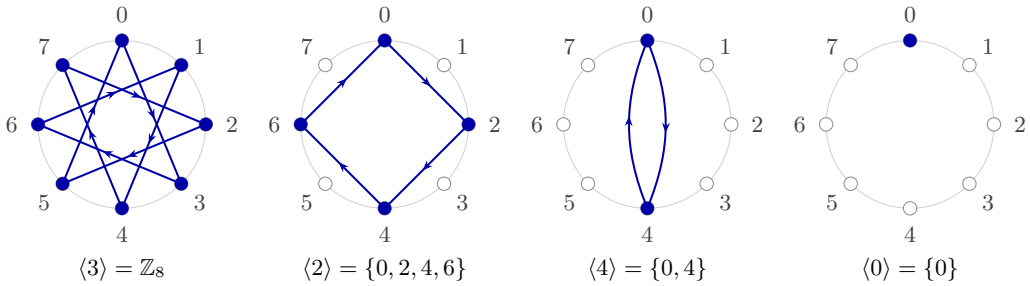


Figure 1: Each cyclic subgroup of $\mathbb{Z}_8$ as a walk round the eight classes, written without brackets, taking steps of a from 0 until the walk closes. Filled dots are the classes reached, and they make up $\langle a \rangle$. Steps of 3 visit all eight classes before returning, so $\langle 3 \rangle = \mathbb{Z}_8$. Steps of 2 visit only the even classes, steps of 4 only 0 and 4, and steps of 0 never leave 0. Steps of 5, 6 and 7 trace the same walks as steps of 3, 2 and 1, run backwards, which is why $\langle a \rangle = \langle a^{-1} \rangle$.

Cyclic groups

The group $(G, *)$ is **cyclic** if there exists an $a \in G$ such that $\langle a \rangle = G$.

Such an a is a **generator** of G. Every element of a cyclic group is a power of the one element a. By the last section, $(\mathbb{Z}_8, +)$ is cyclic, with four generators. More on cyclic groups is in subgroups-and-cyclic-groups[9].

[8] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[9] courses/math1061/subgroups-and-cyclic-groups.pdf

Worked: which of these groups are cyclic?

Which of the following groups are cyclic? $(\mathbb{Z}_{10}, +)$, $(\mathbb{Z}_5 - \{[0]\}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$.

Group	Cyclic?	Generator
$(\mathbb{Z}_{10}, +)$	**yes**	$[1]$
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	**yes**	$[2]$
$(\mathbb{Z}, +)$	**yes**	1
$(\mathbb{Q}, +)$	**no**	none

$(\mathbb{Z}_{10}, +)$. The multiples of $[1]$ are $[1], [2], \dots, [9], [10] = [0]$, all ten classes. So $\mathbb{Z}_{10} = \langle [1] \rangle$.

$(\mathbb{Z}_5 - \{[0]\}, \cdot)$. The set is $\{[1], [2], [3], [4]\}$ and the operation is multiplication, so here powers really are powers. $\langle [1] \rangle = \{[1]\}$, since $[1]$ is the identity. Trying $[2]$:

$$[2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [8] = [3], \quad [2]^4 = [16] = [1].$$

So $\langle [2] \rangle = \{[2], [4], [3], [1]\} = \mathbb{Z}_5 - \{[0]\}$, and the group is cyclic. A generator only has to exist; $[1]$ failing does not matter.

$(\mathbb{Z}, +)$. In additive notation 1^n is n copies of 1 added together, $1^0 = 0$, and $1^{-1} = -1$. So

$$\langle 1 \rangle = \{1^n : n \in \mathbb{Z}\} = \{\dots, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, \dots\} = \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}.$$

An infinite group can be cyclic.

$(\mathbb{Q}, +)$. To show no generator exists, take an arbitrary rational r and find a rational that is not in $\langle r \rangle$. In $(\mathbb{Q}, +)$, $\langle r \rangle = \{kr : k \in \mathbb{Z}\}$, the integer multiples of r.

- *If* $r = 0$, then $\langle 0 \rangle = \{0\}$, which is not $\mathbb{Q}$.
- *If* $r \neq 0$, write $r = \frac{p}{q}$ with $p, q \in \mathbb{Z}$, $q \neq 0$. Then $\frac{p}{2q} = \frac{r}{2}$ is rational. If it were in $\langle r \rangle$ there would be a $k \in \mathbb{Z}$ with $\frac{r}{2} = kr$, and dividing by $r \neq 0$ gives $k = \frac{1}{2}$, which is not an integer. So $\frac{p}{2q} \notin \langle \frac{p}{q} \rangle$.

Either way $\langle r \rangle \neq \mathbb{Q}$, so $(\mathbb{Q}, +)$ is not cyclic. The case $r = 0$ has to be split off because $\frac{0}{2q} = 0$ *is* in $\langle 0 \rangle$. On the number line, $\langle r \rangle$ is a row of equally spaced points, and $\frac{r}{2}$ sits in the first gap (subgroups-and-cyclic-groups[10] draws it).

[10] courses/math1061/subgroups-and-cyclic-groups.pdf

Worked: $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic

> Consider the group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ where $(a,b)+(c,d) = ((a+c) \bmod 2,\ (b+d) \bmod 3)$. Show that this group is cyclic.

The elements are the six pairs (a,b) with $a \in \{0,1\}$ and $b \in \{0,1,2\}$, and the operation adds each coordinate in its own modulus. Try $(a,b) = (1,1)$, adding $(1,1)$ each time:

$$
\begin{aligned}
(1,1)^1 &= (1,1) \\
(1,1)^2 &= (1,1) + (1,1) = (2 \bmod 2,\ 2 \bmod 3) = (0,2) \\
(1,1)^3 &= (1,1)^2 + (1,1) = (0,2) + (1,1) = (1 \bmod 2,\ 3 \bmod 3) = (1,0) \\
(1,1)^4 &= (1,0) + (1,1) = (0,1) \\
(1,1)^5 &= (0,1) + (1,1) = (1,2) \\
(1,1)^6 &= (1,2) + (1,1) = (0,0)
\end{aligned}
$$

The six powers are six different pairs, so they are all of $\mathbb{Z}_2 \times \mathbb{Z}_3$, and

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle. \qquad //$$

Not every element works. $(1,0)$ only reaches $(1,0)$ and $(0,0)$, and $(0,1)$ only reaches the three pairs with first coordinate 0. $(1,1)$ works because its first coordinate cycles with period 2 and its second with period 3, and the two are not back at $(0,0)$ together until the sixth step. The three cyclic subgroups are drawn side by side in subgroups-and-cyclic-groups[11].

The definition of a field

> **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 $(f + g) \cdot h = (f \cdot h) + (g \cdot h)$.

Condition (3) is the pair of **distributive laws**. They are the only condition that involves both operations at once; without them $+$ and $\cdot$ would be two unrelated groups that happen to share a set.

Condition (1) is five checks: closure, associativity, identity and inverses for $+$, and commutativity to make it abelian. Condition (2) is the same five for $\cdot$, on the smaller set $F - \{0\}$. The "0"

[11] courses/math1061/subgroups-and-cyclic-groups.pdf

there means the additive identity, whatever it is called in F; in $\mathbb{Z}_n$ it is $[0]$. Why it has to be removed, and a picture of the two groups, are in fields[12].

Fields already in use

$(\mathbb{R}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are fields. Arithmetic in them uses both kinds of inverse:

- **subtraction** is adding an additive inverse, $a - b = a + (-b)$;
- **division** is multiplying by a multiplicative inverse, $a \div b = a \cdot b^{-1}$ for $b \neq 0$.

Example. Solve $2x + 3 = 8$ in $\mathbb{R}$. Add -3 to both sides to get $2x = 5$, then multiply both sides by $2^{-1} = \frac{1}{2}$ to get $x = \frac{5}{2}$.

Those two steps are all that solving a linear equation needs, and the field axioms are what guarantee they can be done. The same two steps work in any field, including those where -3 and 2^{-1} are classes mod p.

Worked: is $(\mathbb{Z}_4, +, \cdot)$ a field?

> Is $(\mathbb{Z}_4, +, \cdot)$ a field?

No. Condition (1) holds but condition (2) fails.

(1) $(\mathbb{Z}_4, +)$ is an abelian group with identity $[0]$. From the table: closure (only $[0], \ldots, [3]$ appear), associativity (inherited from addition of integers), identity $[0]$ (its row and column repeat the headings), inverses ($[0]$ is in every row: $-[1] = [3]$, $-[2] = [2]$, $-[3] = [1]$), and commutative (the table is symmetric about its diagonal).

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[\mathbf{0}]$	$[0]$	$[1]$	$[2]$	$[3]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[3]$	$[0]$
$[\mathbf{2}]$	$[2]$	$[3]$	$[0]$	$[1]$
$[\mathbf{3}]$	$[3]$	$[0]$	$[1]$	$[2]$

(2) $(\mathbb{Z}_4 - \{[0]\}, \cdot)$ is not a group. The set is $\{[1], [2], [3]\}$:

$\cdot$	$[1]$	$[2]$	$[3]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[3]$
$[\mathbf{2}]$	$[2]$	$[\mathbf{0}]$	$[2]$
$[\mathbf{3}]$	$[3]$	$[2]$	$[1]$

[12] courses/math1061/fields.pdf

$\cdot$	$[1]$	$[2]$	$[3]$

$[2] \cdot [2] = [4] = [0]$, and $[0] \notin \mathbb{Z}_4 - \{[0]\}$. **Closure fails.** Two non-zero classes multiply to zero. The same row shows a second failure: the row of $[2]$ has no $[1]$ in it, so $[2]$ has no multiplicative inverse either.

Worked: which of these is a field?

Two rules to use:

- $(\mathbb{Z}_n, +)$ **is a group for every** $n \in \mathbb{Z}^+$ (integers-modulo-n[13]). It is abelian, so condition (1) always holds for $\mathbb{Z}_n$.
- $(\mathbb{Z}_p, +, \cdot)$ **is a field when** p **is prime.** Why, and why a composite n never works, is in fields[14].

Which of the following is a field? (a) $(\mathbb{Z}, +, \cdot)$ (b) $(\mathbb{Z}_7, +, \cdot)$ (c) $(\mathbb{Z}_{15}, +, \cdot)$

(a) $(\mathbb{Z}, +, \cdot)$**: not a field.**

1. $(\mathbb{Z}, +)$ is an abelian group with identity 0. ✓
2. $(\mathbb{Z} - \{0\}, \cdot)$ is not a group, because 2 has no inverse: the identity is 1, and $2 \cdot y = 1$ needs $y = \frac{1}{2} \notin \mathbb{Z}$. ×

So $(\mathbb{Z}, +, \cdot)$ is not a field. This is where the second step of solving an equation breaks down in $\mathbb{Z}$: there is no 2^{-1} to multiply $2x = 5$ by, and indeed no integer x has $2x = 5$.

(b) $(\mathbb{Z}_7, +, \cdot)$**: a field,** since 7 is prime. Checking each condition directly:

1. $(\mathbb{Z}_7, +)$ is an abelian group with identity $[0]$, by the first rule. ✓
2. $(\mathbb{Z}_7 - \{[0]\}, \cdot)$ is the abelian group whose table is worked in 2026-09-24-definitions-and-examples-of-groups[15]. Its inverses are $[1]^{-1} = [1]$, $[2]^{-1} = [4]$, $[3]^{-1} = [5]$, $[6]^{-1} = [6]$. ✓
3. The distributive laws are inherited from the integers: $[a] \cdot ([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$, and the other law follows the same way. ✓

(c) $(\mathbb{Z}_{15}, +, \cdot)$**: not a field.**

1. $(\mathbb{Z}_{15}, +)$ is an abelian group with identity $[0]$. ✓
2. $(\mathbb{Z}_{15} - \{[0]\}, \cdot)$ is not a group: $[3] \cdot [5] = [15] = [0]$, which is not in the set, so closure fails. ×

[13] courses/math1061/integers-modulo-n.pdf
[14] courses/math1061/fields.pdf
[15] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

So $(\mathbb{Z}_{15}, +, \cdot)$ is not a field. The factorisation $15 = 3 \cdot 5$ is exactly what produces the two non-zero classes with product [0].

Solving equations in a field

In a field, a linear equation is solved exactly as in $\mathbb{R}$: add the additive inverse of the constant to both sides, then multiply both sides by the multiplicative inverse of the coefficient. In $\mathbb{Z}_p$ both inverses are classes, and the multiplicative one has to be found. The general method, with a picture, is in fields[16].

Worked: linear equations in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{17}$

> **(a)** Solve the equation $2x + 3 = 8$ in the field $(\mathbb{Z}_{11}, +, \cdot)$. Hence determine the smallest positive integer y such that $2y + 3 \equiv 8 \pmod{11}$.
>
> **(b)** Solve the equation $10x + 9 = 6$ in the field $(\mathbb{Z}_{17}, +, \cdot)$. Hence determine the smallest positive integer y such that $10y + 9 \equiv 6 \pmod{17}$.

(a) Work mod 11, writing 2 for [2] and so on inside the equation.

$$
\begin{aligned}
2x + 3 &= 8 && \\
2x + 3 + (-3) &= 8 + (-3) && \text{add the additive inverse of 3, } [-3] = [8] \\
2x &= 5 && \\
6 \cdot 2x &= 6 \cdot 5 && \text{multiply by the multiplicative inverse of 2, which is 6} \\
[12]x &= [30] && \\
1 \cdot x &= 8 && [12] = [1] \text{ and } [30] = [8] \\
x &= [8] &&
\end{aligned}
$$

The inverse of [2] is [6] because $2 \cdot 6 = 12 \equiv 1 \pmod{11}$.

Check: $2(8) + 3 = 19 \equiv 8 \pmod{11}$. ✓

The integers y with $2y + 3 \equiv 8 \pmod{11}$ are exactly the members of the solution class $[8] = \{\dots, -14, -3, 8, 19, 30, \dots\}$. The smallest positive one is $\mathbf{y = 8}$.

(b) Work mod 17.

[16] courses/math1061/fields.pdf

$$
\begin{aligned}
10x + 9 &= 6 && \\
10x + 9 + (-9) &= 6 + (-9) && \text{add the additive inverse of 9, } [-9] = [8] \\
10x &= -3 && \\
12 \cdot 10x &= 12 \cdot (-3) && \text{multiply by the multiplicative inverse of 10, which is 12} \\
1 \cdot x &= -36 && [120] = [1] \\
x &= [-36] = [-2] = [15] && -36 = (-2) \cdot 17 - 2
\end{aligned}
$$

Finding $[10]^{-1}$. In part (a) the inverse of $[2]$ could be seen at once from $2 \cdot 6 = 12$. Here it takes a search: list the multiples of 10 mod 17 until one is $\equiv 1$. Each line is the previous one plus 10, with 17 taken off whenever the total passes 16:

k	1	2	3	4	5	6	7	8	9	10	11	12
$10k \bmod 17$	10	3	13	6	16	9	2	12	5	15	8	**1**

$10 \cdot 12 = 120 = 7 \cdot 17 + 1$, so $[10]^{-1} = [12]$. Along the way, $10 \cdot 5 = 50 \equiv 16 = -1$, which is another route: $[10]^{-1} = -[5] = [12]$.

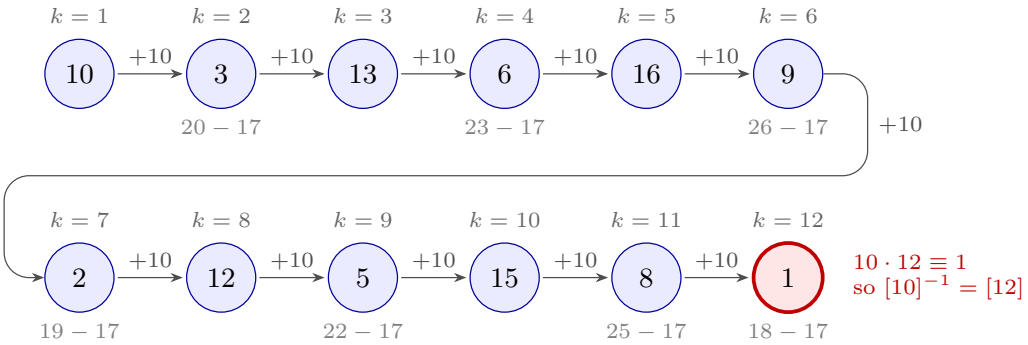


Figure 2: Searching for the inverse of $[10]$ in $\mathbb{Z}_{17}$. Starting at 10, each hop adds 10 and reduces mod 17; the grey number under a class is the unreduced total, shown where 17 had to be taken off. Because 17 is prime, the hops pass through non-zero classes only and cannot repeat before every non-zero class has appeared, so the class 1 is certain to turn up. It turns up at the twelfth multiple, so $10 \cdot 12 \equiv 1 \pmod{17}$ and $[10]^{-1} = [12]$.

Reducing the answer. $-36 = (-2) \cdot 17 - 2$, so $[-36] = [-2]$, and $[-2] = [-2 + 17] = [15]$. A shorter path is to notice $[12] = [-5]$, so $x = [-5] \cdot [-3] = [15]$ straight away.

Check: $10(15) + 9 = 159 = 10 \cdot 17 - 11 \equiv -11 \equiv 6 \pmod{17}$. ✓

The integers y with $10y + 9 \equiv 6 \pmod{17}$ are the members of $[15] = \{\dots, -19, -2, 15, 32, \dots\}$. The smallest positive one is $\mathbf{y = -2 + 17 = 15}$. The representative -2 is a correct name for the class, but it is not the positive integer the question asks for.

See also

- fields[17] — the definition, examples and non-examples, why $\mathbb{Z}_n$ is a field exactly when n is prime, and solving equations
- subgroups-and-cyclic-groups[18] — subgroups, $\langle a \rangle$, and cyclic groups
- integers-modulo-n[19] — $\mathbb{Z}_n$, and multiplicative inverses mod p
- groups[20] — the four group properties used in conditions (1) and (2)
- cayley-tables[21] — reading closure and inverses off a table, as in the $\mathbb{Z}_4$ question
- 2026-10-06-elementary-properties-of-groups[22] — Lecture 27 · 2026-10-12-introduction-to-counting[23] — Lecture 29
- practice-problems[24] — §34, where Q4 shows that $(\mathbb{Z}_{11} - \{[0]\}, \cdot)$ is cyclic
- practice-problems[25] — §36, with full worked solutions

[17] courses/math1061/fields.pdf
[18] courses/math1061/subgroups-and-cyclic-groups.pdf
[19] courses/math1061/integers-modulo-n.pdf
[20] courses/math1061/groups.pdf
[21] courses/math1061/cayley-tables.pdf
[22] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[23] courses/math1061/2026-10-12-introduction-to-counting.pdf
[24] courses/math1061/practice-problems.pdf
[25] courses/math1061/practice-problems.pdf