Linear System Theory.

Exercise

Equivalent classes
and finite fields

$\mathbb{Z}/5\mathbb{Z}$

$\mathbb{Z}/5\mathbb{Z}$: $\quad \overline{0} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$

infinite sets $\quad \overline{1} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$

$\overline{2} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$

$\overline{3} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$

$\overline{4} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$

and stop since $\overline{5} = \overline{0}$

multiplication table (we omit $\overline{a}$, i.e. a $\quad \overline{0} = 0 \quad \overline{1} = 1$ etc.)

multiplication in $\mathbb{Z}/5\mathbb{Z}$:

$\perp$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$1 = \overline{1}$ neutral element $\mathbb{1}$

Because 1 appears only once on every column and line, it is a field.

A few checks: $\overline{4} \top \overline{4}$:

$$-6 \cdot 9 = -54 = -5 \cdot 11 + 1 \equiv 1 \mod 5$$

$-6 \in \overline{4}$

$9 \in \overline{4}$ $\quad (-54 \in \overline{1})$ $\quad \Rightarrow \overline{4} \top \overline{4} = \overline{1}$

$\overline{2} \perp \overline{3}$:

$$12 \cdot 3 = 36 = 5 \cdot 7 + 1 \equiv 1 \mod 5$$

$$\Rightarrow \quad \overline{2} \perp \overline{3} = \overline{1}$$

etc...