Last time:

We defined cosets of a subring $S$ of a ring $R$.

Two elements $a, b \in R$ are related by:

$$a \sim_S b \text{ if and only if } a - b \in S$$

The equivalence classes

$$[a]_S = \{ b \in R \mid a - b \in S \}$$
$$\shortparallel$$
$$a + S$$

are the cosets of $S$ in $R$.

---

Proposition Suppose $S$ is a subring of the ring $R$.
Take any coset $a + S$.
The function

$$\sigma : S \longrightarrow a + S$$
$$s \longmapsto a + s.$$

is a bijection

Proof: We must show that $\sigma$ is both injective and surjective.

Surjective: Take any element $b \in a + S$. This means $b = a + s$ with $s \in S$. Then $\sigma(s) = a + s = b$.

**Injective**: Suppose $\tau(s_1) = \tau(s_2)$ for $s_1, s_2 \in S$.

$$a + s_1 = a + s_2$$

By the cancellative law,

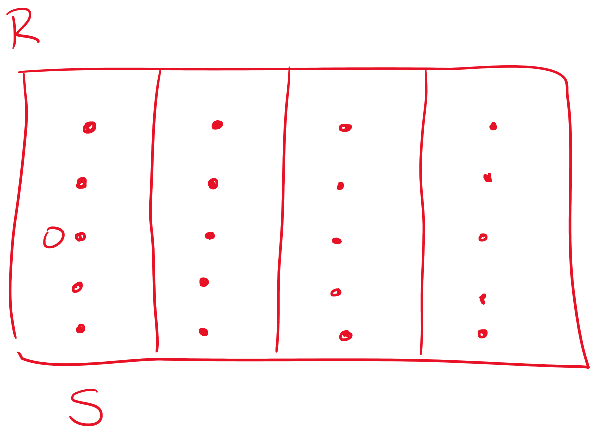
$$s_1 = s_2.$$

---

**Corollary**: If $S$ is a finite subring of $R$ then all the cosets of $S$ in $R$ have the same number of elements (equal to $|S|$). If $R$ is finite, there are $|R|/|S|$ many cosets.

---

Picture




$|R| = 20$

$|S| = 5$

$|R|/|S| = 4$ cosets.

---

**Corollary**: A subring $S$ of a ring $R$ must satisfy $|S|$ divides $|R|$.

---

# Homomorphisms:

A **homomorphism** between two rings $R$ and $T$ is a function

$$f : R \longrightarrow T$$

satisfying

$$f(\underbrace{a+b}_{\text{addition in } R}) = f(a) \underbrace{+}_{\text{addition in } T} f(b)$$

$$f(\underbrace{a\cdot b}_{\text{multiplication in } R}) = f(a) \underbrace{\cdot}_{\text{multiplication in } T.} f(b)$$

for any $a, b \in R$.

---

**Examples:** Consider the function

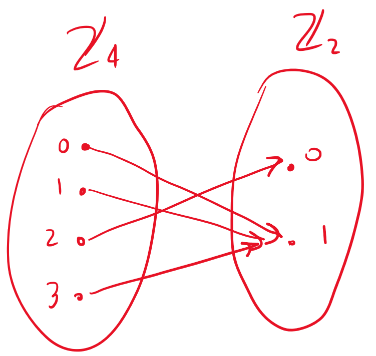
$$f : \underbrace{\mathbb{Z}_4}_{\text{integers mod } 4} \longrightarrow \underbrace{\mathbb{Z}_2}_{\text{integers mod } 2.}$$

$$[0]_4 \longmapsto [1]_2$$

$$[1]_4 \longmapsto [1]_2$$

$$[2]_4 \longmapsto [0]_2$$

$$[3]_4 \longmapsto [1]_2 .$$




Not a homomorphism.

Is this a homomorphism?

No, because for instance

$$f([0]_4 + [2]_4) = f([2]_4) = [0]_2$$

$$\#$$

$$f([0]_4) + f([2]_4) = [1]_2 + [0]_2 = [1]_2$$

The function

$$g : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$$

$$[0]_4 \longmapsto [0]_2$$

$$[1]_4 \longmapsto [1]_2$$

$$[2]_4 \longmapsto [0]_2$$

$$[3]_4 \longmapsto [1]_2$$

This is a homomorphism of rings.

(this requires an argument!).

Another homomorphism:

$$h : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2$$

$$[0]_4 \longmapsto [0]_2$$

$$[1]_4 \longmapsto [0]_2$$

$$[2]_4 \longmapsto [0]_2$$

$$[3]_4 \longmapsto [0]_2$$

This is called the "trivial" homomorphism.

## Challenge problem.

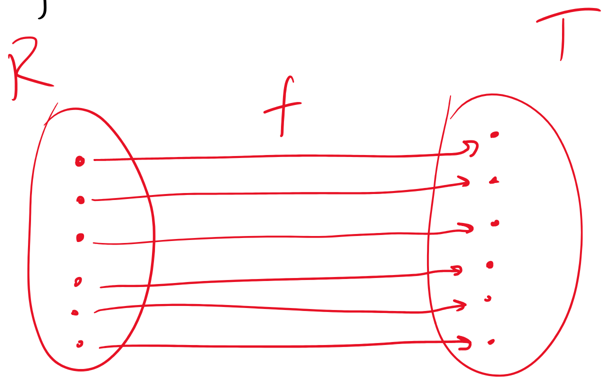
- What are all possible homomorphisms between

$$\mathbb{Z}_{12} \longrightarrow \mathbb{Z}_4 \; ?$$

In general: $\mathbb{Z}_m \longrightarrow \mathbb{Z}_n$ ?

---

**Definition.** An <u>isomorphism</u> between rings $R$ and $T$ is a bijection that is a homomorphism.




In other words, the rings $R$ and $T$ are "the same ring but with different names for the elements".

---

## Exercises:

- Let's figure out whether $\mathbb{Z}_2$ and $\mathcal{P}(\{a\})$ are isomorphic rings.

$$\mathbb{Z}_2 = \{0, 1\}$$

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| · | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

$$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$$

| + | $\emptyset$ | $\{a\}$ |
|---|---|---|
| $\emptyset$ | $\emptyset$ | $\{a\}$ |
| $\{a\}$ | $\{a\}$ | $\emptyset$ |

| · | $\emptyset$ | $\{a\}$ |
|---|---|---|
| $\emptyset$ | $\emptyset$ | $\emptyset$ |
| $\{a\}$ | $\emptyset$ | $\{a\}$ |

Looking at these tables, we see that the rings are isomorphic:

$$\mathbb{Z}_2 \longrightarrow \mathcal{P}(\{a\})$$

$$0 \longmapsto \emptyset$$

$$1 \longmapsto \{a\}$$

**Exercise 1:** Are $\mathbb{Z}_4$ and $\mathcal{P}(\{a,b\})$ isomorphic? Explain.

**Exercise 2:** List all the subrings of $\mathbb{Z}_{12}$.

**Answers:**

(1)

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | | | | |
| 1 | | 2 | | |
| 2 | | | | |
| 3 | | | | |

| + | $\emptyset$ | $\{a\}$ | $\{b\}$ | $\{a,b\}$ |
|---|---|---|---|---|
| $\emptyset$ | | | | |
| $\{a\}$ | | $\emptyset$ | | |
| $\{b\}$ | | | | |
| $\{a,b\}$ | | | | |

Not the same table, and not even after reordering the elements: In $\mathcal{P}(\{a,b\})$, $x+x=0$ for all $x$, while this is not the case in $\mathbb{Z}_4$.

(2) $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$

$S_{12} = \{0\}$

$$S_6 = \{0, 6\}$$

$$S_4 = \{0, 4, 8\}$$

$$S_3 = \{0, 3, 6, 9\}$$

$$S_2 = \{0, 2, 4, 6, 8, 10\}$$

$$S_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

There are 6 subrings because there are 6 divisors of 12.

Diagram of all the subrings taking into account containment between them: