Example 1.8. Let $M_{2\times 2}\mathbb{R}$ denote the set of 2×2 matrices with real entries. This is a group under addition, but is *not* a group under matrix multiplication, because some matrices are not invertible (e.g. the zero matrix).

Example 1.9. The **general linear group** of 2×2 matrices is

$$GL_2(\mathbb{R}) = \{A \in M_{2\times 2}(\mathbb{R}) \mid \det A \neq 0\}.$$

By definition[2], everything in $GL_2(\mathbb{R})$ has a multiplicative inverse. Matrix multiplication is indeed associative. We write either I or I_2 for the identity matrix.

1.2 Groups as sets of symmetries

Historically, groups came up naturally from *group actions*. The action corresponding to the identity element is "do nothing".

To me, the most concrete way to understand and see a group action is to think about symmetries of 2D regular polygons.

Question 1.10. What are the *symmetries* of a square? How many different symmetries are there?

If we think of a square as a rigid object, we can rotate it by angles that are multiples of $\pi/2$, and also reflect across vertical, horizontal, and diagonal (angle $\pm\pi/4$) lines.

Suppose we are building a video game where you need to be able to manipulated a square with only two buttons. We might choose to assign our buttons to the following actions:

- $\rho =$ rotate by $\pi/2$ CCW (counterclockwise)
- $\tau =$ reflect across the x-axis

We think about actions like we think about functions (hence the $\circ$ symbol).

Question 1.11. Can you write down a sequence of button presses to achieve all the symmetries of the square?

There are obviously many different sequences of button presses that would achieve the same result. One important but perhaps non-obvious way to do absolutely nothing is $\rho \circ \tau \circ \rho \circ \tau = (\rho \circ \tau)^2$. (Try it!)

Definition 1.12. The **dihedral group** D_n is the group of symmetries of a regular n-gon. [3]

One way we will use to describe groups is called **group presentation**, which is written in the form

$$\langle \text{generators} \mid \text{relations} \rangle.$$

The generators are the buttons you implement. The relations are a set of button presses that do nothing. Once we understand *normal subgroups*, we will be able to formalize this definition rigorously. However, it's still useful to us right now, for intuition. For example, we can describe the set of symmetries of a square now as

$$D_4 = \langle \rho, \tau \mid \rho^4 = \tau^2 = \rho\tau\rho\tau = 1 \rangle.$$

Remark 1.13. Notice that I've been eliding the composition symbol $\circ$ in favor of *multiplicative notation*. We will talk more about conventions later, but for now you should just think back to how you used to write $2 \times 2 = 4$, then you started writing $a \cdot b = c$, and even later on you would just write $AB = I$.

Exercise 1.14. Write down a group presentation for the symmetries of a triangle: define what your generators do, and then write down some obvious relations. Then, think about how you would prove that your presentation uniquely determines your symmetry group D_3.

[2] review determinants if this isn't clear!

[3] Warning: There are other conventions; some people write D_{2n} instead.

1.3 Cyclic groups C_n

Definition 1.15. A group G is **cyclic** if it is generated by a single element, i.e. there exists an element $\rho \in G$ such that every $g \in G$ can be written in the form $g = \rho^k$ for some $k \in \mathbb{Z}$.

Example 1.16. The cyclic group C_{12} has the presentation

$$C_{12} = \langle \rho \mid \rho^{12} = 1 \rangle.$$

Question 1.17. Is $\mathbb{Z} = (\mathbb{Z}, +)$ a cyclic group?

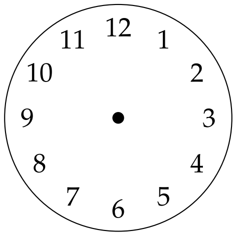
Definition 1.18. The **order** of a group G is the number of elements that it contains, and is denoted $|G|$.

- If $|G|$ is finite, then G is a *finite group*.
- If $|G|$ is infinite, then G is an *infinite group*.

Question 1.19. What is the order of the group $C_n = \{\rho \mid \rho^n = 1\rangle$?

Exercise 1.20. Prove that every cyclic group is abelian.

Example 1.21. While we used multiplicative notation above to define C_{12}, this group is basically the same as the additive group we use when we look at analog clocks:



The group $\mathbb{Z}/12\mathbb{Z}$ is the additive group of integers **mod 12**. (We will talk more about this notation later.)

The group operation, addition, works exactly as you'd expect while looking at a 12-hour analog clock. For example, 8 am + 6 hours = 2 pm, so 8 + 6 = 2.

This brings us to an important point about additive and multiplicative notation.

Remark 1.22. (Notation Conventions)

So far in this class we've used a couple different notations for the **composition law / group operation** in a group G:

1. An abstract symbol, such as $\circ$.
   - Permutations $p, q \in S_n$ are set maps $[n] \to [n]$. We can compose them in two ways: $p \circ q$ or $q \circ p$.
   - When $n \geq 3$, S_n is **nonabelian**, so in general $p \circ q \neq q \circ p$.
2. **Additive notation**, where $+$ is a **commutative** group operation:
   - e.g. $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$
   - Use 0 to represent the **additive identity**.
3. **Multiplicative notation**, where $b \circ a = b \cdot a$ is written ba:
   - If $x, y \in \mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$, we write xy as their product.
   - If $p, q \in S_n$, we write pq or qp. In general, $pq \neq qp$.
   - Use 1 to represent the **multiplicative identity**.