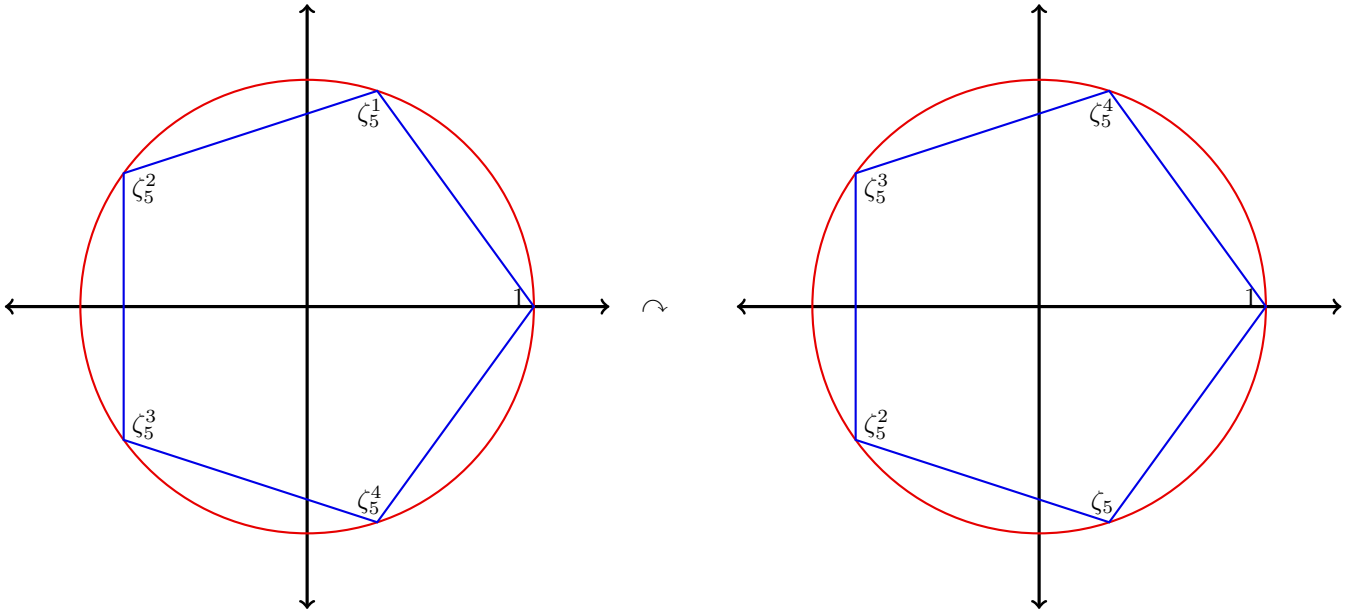
MATH 3311, FALL 2025: LECTURE 4, SEPTEMBER 3

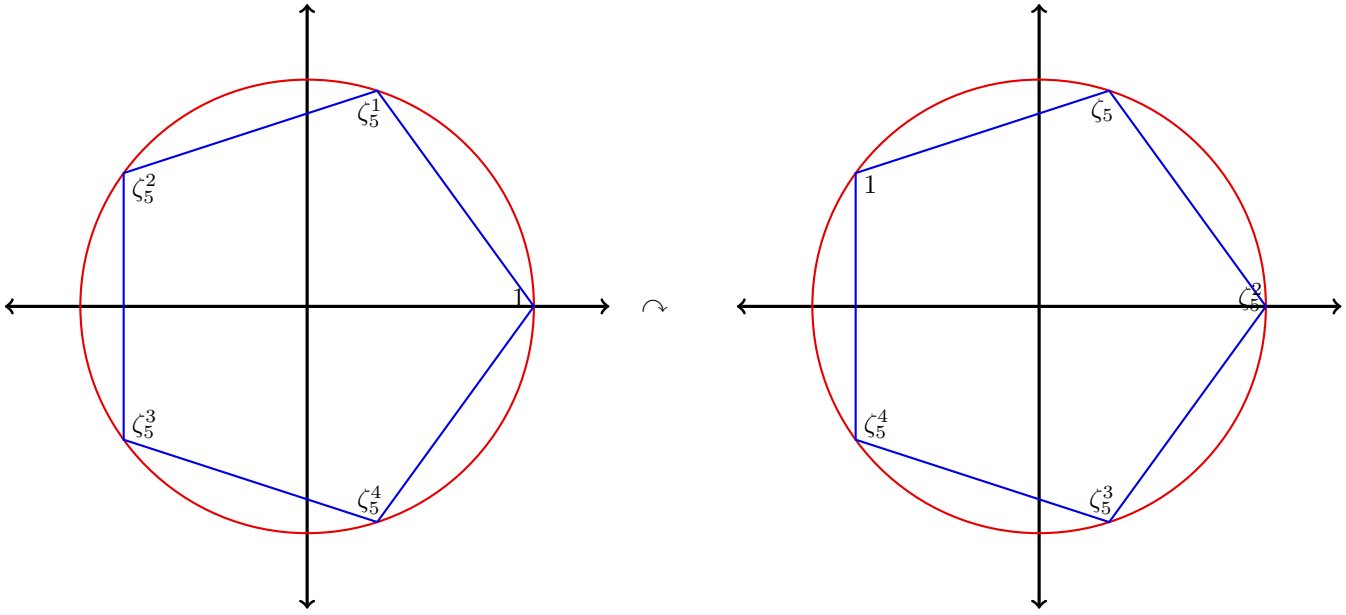
Video: `https://youtu.be/rynVz1lw65o`

Recall from last time the set of *rigid symmetries* of the regular pentagon in the plane. We'll refer to this set by D_{10}, since as we will see below it has exactly 10 elements.



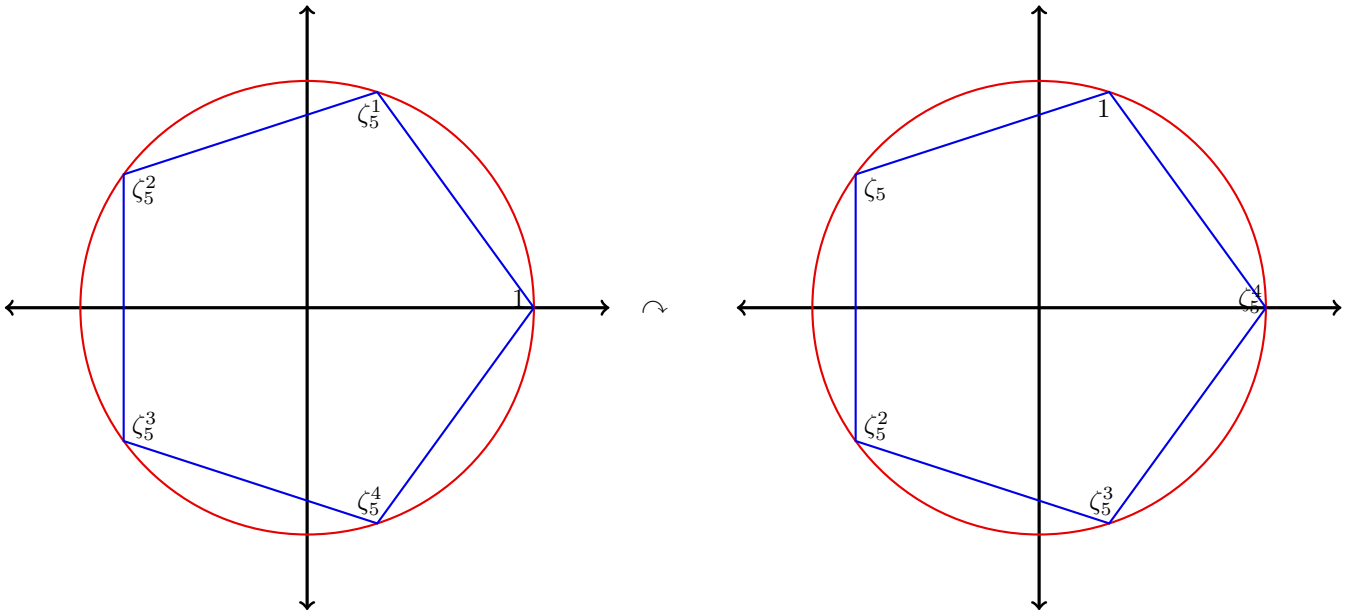
This fixes 1 and flips the other four in pairs.

But we could also reflect it across the median through ζ_5.



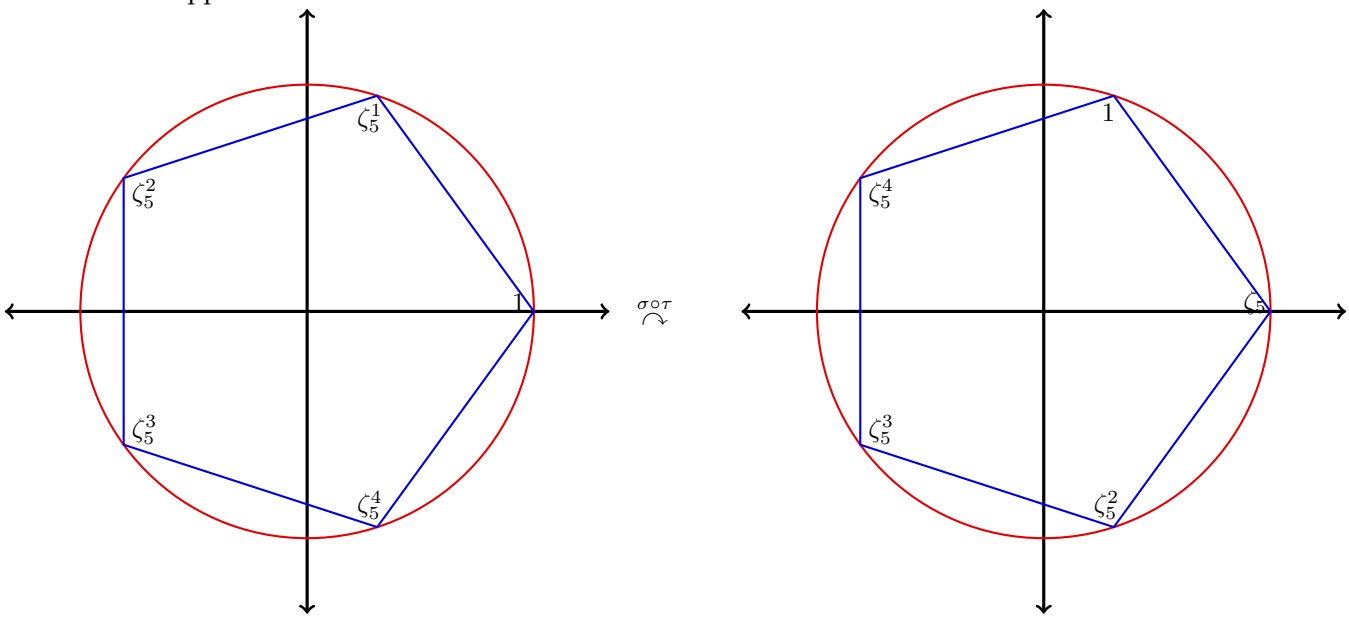
This fixes ζ_5 and flips 1 with ζ_5^2, and ζ_5^3 with ζ_5^4.

Another thing we can do is rotate everything by some integer multiple of $2\pi/5$. For instance, if we rotate counterclockwise by $2\pi/5$, we get:



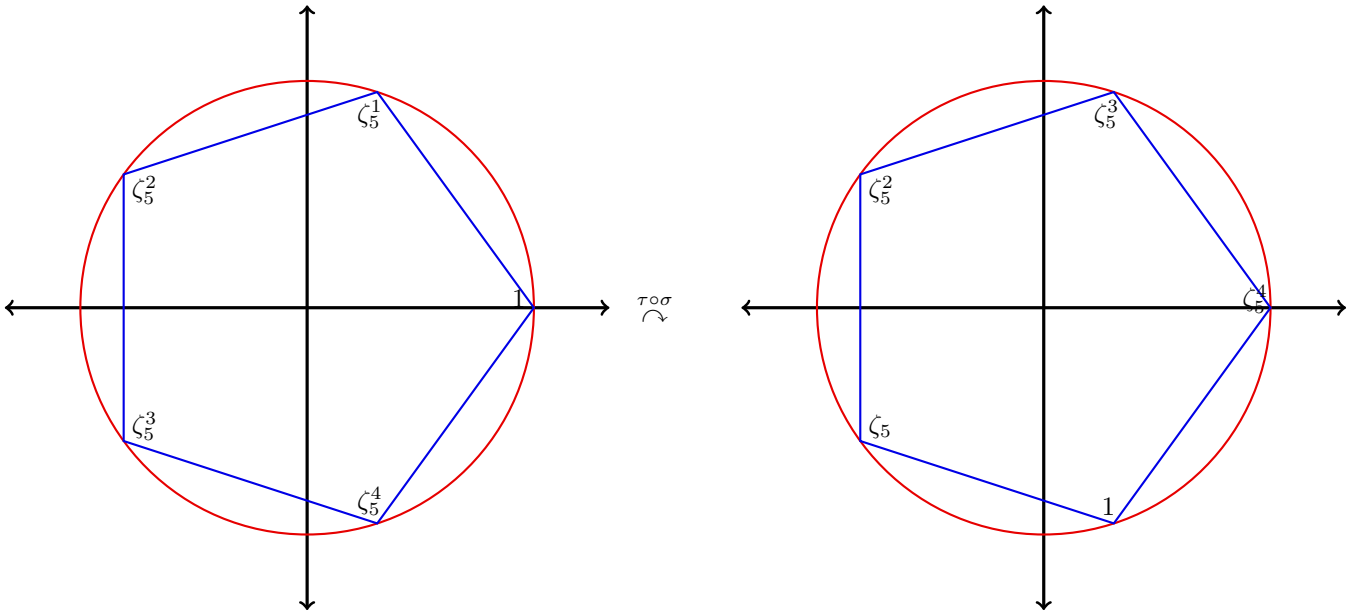
Let us call this rotation σ, and let us write τ for the complex conjugation symmetry (or reflection across the median through 1) from the beginning.

Here is what happens when we do τ first and then σ:



This is just reflection across the median through ζ_5^3!

On the other hand, here is what happens when we look at σ followed by τ:



This is actually reflection across the median through ζ_5^2![1]. Therefore, we see that $\sigma \circ \tau \neq \tau \circ \sigma$: the order of composition matters!

Remark 1. In general, the composition of any two rigid symmetries, rotation or reflection, will produce another rigid symmetry: There are five reflections and five rotations (including the *trivial* rotation by 2π or 0), giving a total of 10 rigid symmetries of the regular pentagon. Therefore, we will denote this set by D_{10}. You can repeat this analysis for any regular n-gon and get a set of $2n$ rigid symmetries that we denote by D_{2n}.

Okay, it is time for our first definition of this class.

Definition 1. A **group** is a triple $(G, *, e)$, where:

- G is a set;
- $*$ is a (binary) operation

$$G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 * g_2$$

- $e \in G$ is an element

that satisfy the following properties:

(1) (Identity) For all $g \in G$, we have

$$e * g = g * e = g.$$

We call e the **identity** element of G.

(2) (Associativity) For all $g_1, g_2, g_3 \in G$, we have[2]

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$

(3) (Inverse) For every $g \in G$, there exists $h \in H$ such that

$$g * h = e.$$

Let us now look at some examples of groups.

Example 1. The first example is the **group with one element** or **trivial group**: We have $G = \{e\}$, the element e is the identity and the operation is given by $e * e = e$.

[1] In the lecture, I said this was reflection through ζ_5^4, which is an error!

[2] The main motivation for what at first glance may seem non-intuitive is that function composition is *always* associative. This is very important.

Example 2. The integers $(\mathbb{Z}, +, 0)$ under addition with 0 as the additive identity. Note that the natural numbers do *not* form a group under addition, because they don't contain inverses for the operation.

Example 3. The real numbers $(\mathbb{R}, +, 0)$ under addition.

Example 4. The non-zero rational numbers $(\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}, \cdot, 1)$ under multiplication.

Example 5. Note that the non-zero *integers* do not form a group under multiplication, because for instance $1/5$ is not an integer. But the two invertible integers $1, -1$ do form a two element group under multiplication.

Example 6. The group of symmetries of the fifth roots of 1 with their multiplicative structure, with the operation being composition. This is a four element group where the order of composition doesn't actually matter.

Example 7. The group D_{10} of rigid symmetries of the regular pentagon with the operation being composition, and where the identity element is given by the trivial rotation. This is a 10 element group where the order of composition *does* matter.

Example 8. The set $\mathbb{Z}/n\mathbb{Z}$ of equivalence classes of integers mod-n equipped with *addition*: the identity is the equivalence class of 0, the bin containing all multiples of n.

Example 9. In Homework 1, you also saw that, when p is a *prime*, the set $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ of non-zero equivalence classes mod-p is a group under *multiplication*: every non-zero equivalence class has a multiplicative inverse.

Homomorphisms

A very important principle in algebra is that what really matters about objects is not always their internal structure, but rather the relations that they exhibit with respect to other objects of the same 'type'. Here is the precise meaning of what this notion means for groups.

Definition 2. Given groups $(G, *_G, e_G), (H, *_H, e_H)$, a **group homomorphism** $f : (G, *_G, e_G) \to (H, *_H, e_H)$ is a function

$$f : G \to H$$

such that, for all $g_1, g_2 \in G_1$, we have

$$f(g_1 *_G g_2) = f(g_1) *_H f(g_2) \in G_2.$$

Note that we are not asking for all the components of the group axiomatics to be respected. For instance, we are not asking for the identity to be respected, or for the inverses, for that matter. It turns out this is not necessary.