Example 2: (back to $\mathbb{Z}_n$)

We know that $\mathbb{Z}_n$ is a group under the binary operation of addition:

$$[a] + [b] = [a+b].$$

However, "$\cdot$" is also a binary operation:

$$[a] \cdot [b] = [a \cdot b].$$

Is $(\mathbb{Z}_n, \cdot)$ a group?

No!

$[0]$ is never invertible with respect to " $\cdot$ ".

Why is this?

Well, if $[a] \in \mathbb{Z}_n$.

$$
\begin{aligned}
[0] \cdot [a] &= [0+0] \cdot [a] \\
&= [(0+0) \cdot a] \\
&= [0 \cdot a + 0 \cdot a] \\
&= [0 \cdot a] + [0 \cdot a] \\
&= [0] \cdot [a] + [0] \cdot [a]
\end{aligned}
$$

Subtract $[0] \cdot [a]$ from both

sides to get

$$[0] \cdot [a] = [0]$$

$\Rightarrow$ in order for $\mathbb{Z}_n$ to be a group under multiplication, $[0]$ would have to be the multiplicative identity, and it is not! The multiplicative identity is $[1]$.

What if we remove $[0]$?

Is $\mathbb{Z}_n \setminus \{[0]\}$ a group with respect to multiplication?

Not in general: it is a group precisely when n is prime.

HW 3 will tell us how to find inverses.

Example 3: (quaternionic basis)

Start with 8 symbols:

$$\{1, -1, i, -i, j, -j, k, -k\} = \mathbb{H}$$

Declare $1 \cdot x = x \cdot 1 = x \quad \forall\, x \in \mathbb{H}$

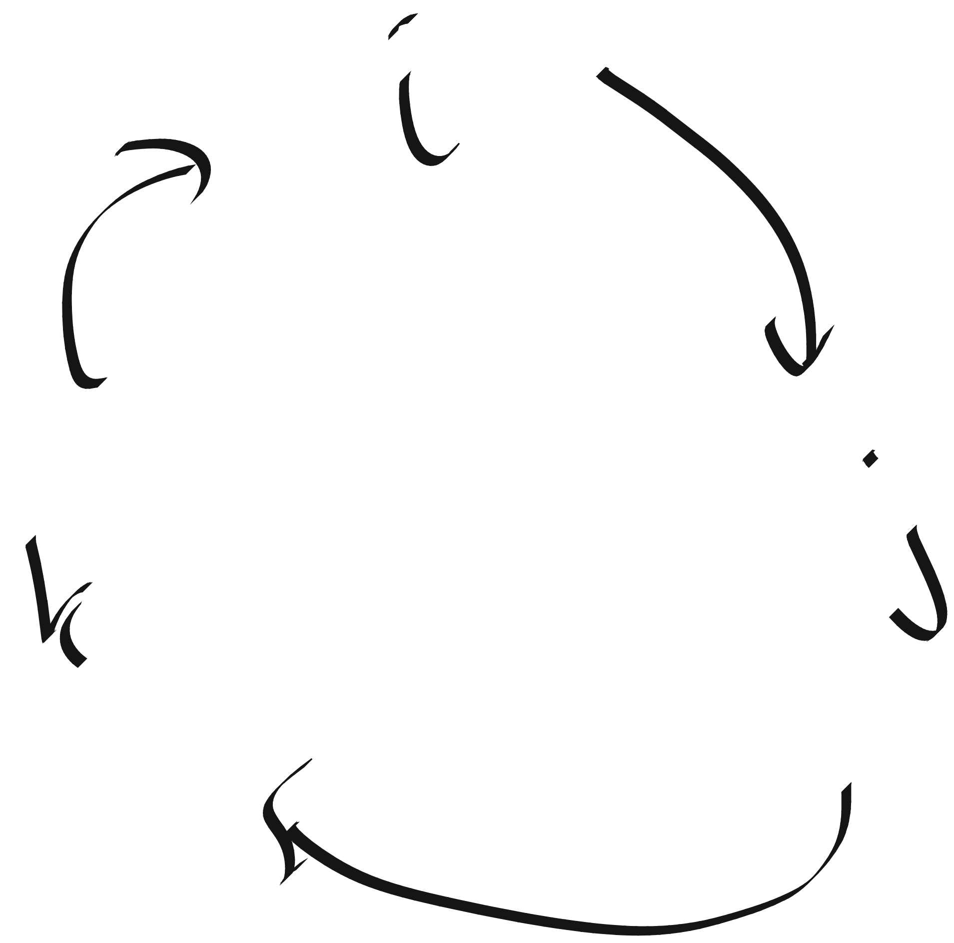
and $(-1) \cdot x = x \cdot (-1) = -x \quad \forall\, x \in \mathbb{H}$

where $-(-1) = 1, \quad -(-j) = j,$

$-(-i) = i, \quad -(-k) = k.$

We now need to know how to "multiply" i's, j's, and k's.

The picture:



$i \cdot j = k$

$j \cdot k = i$

$k \cdot i = j$

$i \cdot i = -1$

$j \cdot j = -1$

$k \cdot k = -1$

$j \cdot i = -k$

$k \cdot j = -i$

$i \cdot k = -j$

Then this multiplication is a binary operation on $\mathbb{H}$.

The identity is 1 by definition.

For inverses,

$$(-j)(j) = (-1)(j)\cdot(j)$$

$$= (-1)(-1)$$

$$= 1$$

Similarly,

$$(j)(-j) = (k)(-k) = i(-i) = (-i)(i) = (-k)\cdot k$$

$$= 1$$

Since $(-1)\cdot(-1)=1$, every element in $\mathbb{H}$ is invertible.

Associativity is a tedious check of the pairings, which we will not do! The cheap way out is to represent $\mathbb{H}$ as matrices with complex entries. This multiplication becomes matrix multiplication, and then we can use associativity of matrix multiplication.

The "$\mathbb{H}$" is for Hamilton, the mathematician who discovered these relations.

Other groups:

- $(\mathbb{Q},+)$ or $(\mathbb{Q}\setminus\{0\},\cdot)$

- $(\mathbb{R},+)$ or $(\mathbb{R}\setminus\{0\},\cdot)$

- $M_n(\mathbb{R})$, the $n\times n$ matrices with real entries, under the operation of component-wise addition

- $GL_n(\mathbb{R})$, the $n\times n$ invertible matrices with real entries, under the operation of matrix multiplication

Definition: (group isomorphism)

Let $(G_1, \cdot)$ and $(G_2, *)$ be groups (the sets are G_1, G_2 with associated binary operations "$\cdot$" and "$*$", respectively.)

A group isomorphism is a function $\varphi : G_1 \to G_2$ such that

1) φ is bijective

2) $\varphi(gh) = \varphi(g) * \varphi(h)$

$\forall \ g, h \in G_1$

φ "distributes" over group multiplication. If such a φ exists, we say G_1 and G_2 are **isomorphic** as groups.

Example 4: (symmetries and S_3)

Let G_1 be the symmetries of an equilateral triangle and G_2 be S_3, both with the operation of function composition. Then these two groups are isomorphic!

Define $\varphi: S_3 \to G_1$ via

$\varphi((1\,2\,3)) = R_{120^\circ}$

$\varphi((1\,3\,2)) = R_{240^\circ}$

$\varphi((1)(2)(3)) =$ do nothing

$\varphi((12)) =$ pick a flip about an axis of symmetry

$\varphi((23)) = ?$

$(23) = (1\ 2)(1\ 2\ 3)$, so

define

$\varphi((23)) = \varphi((12)) \cdot \varphi((123))$

$(1\ 3) = (1\ 2)(1\ 3\ 2)$, so

define

$\varphi((13)) = \varphi((12))\,\varphi((123))$

Q: How do we know φ is injective?

You can either check using where you sent (12) under φ

-or- use the fact that $\varphi((12))$ is invertible,

So if

$\varphi((13)) = \varphi((23))$, then

$$\varphi((12))\,\varphi((132)) = \varphi((12))\,\varphi((123))$$

multiply both sides on the left by $\varphi((12)) = (\varphi((12)))^{-1}$.

We get

$$R_{240^\circ} = \mathcal{C}(((132))) = \mathcal{C}(((123)) = R_{120^\circ}$$

Not equal!

Do this for all relevant pairings (there aren't many).

Distribution over products is a tedious element-by-element check.

Q: Is S_4 isomorphic to the group of symmetries of the square?

A: No! $|S_4| = 4! = 24$, but the number of symmetries of the square is 8, so no bijection between these sets can exist.

Further Q: (dodecagon) Is S_4 isomorphic to the symmetries of a regular dodecagon (12-sided figure)? You can calculate that there are exactly 24 symmetries!

A: Think about it!

Lemma: (invertible elements in $\mathbb{Z}_n$)

In $\mathbb{Z}_n$ with multiplication, $[m]$ is invertible if and only if $\gcd(m,n)=1$.