Groups

Def. A group is a set G
with a binary operation $\cdot : G \times G \to G$
satisfying 3 axioms:

1. associativity: $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ $\forall g, h, k \in G$
2. identity: $\exists e \in G$ such that $g \cdot e = e \cdot g = g$ $\forall g \in G$
3. inverses: $\forall g \in G$ $\exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$

If $g \cdot h = h \cdot g$ for all $g, h \in G$, then G is called **Abelian**

Lemmas:

- e is unique: if e and e' both satisfy (2) then $e = e'$ $\longrightarrow$ $e = e \cdot e' = e'$
- inverses are unique
- $(a^{-1})^{-1} = a$
- if $ab = ac$ then $b = c$

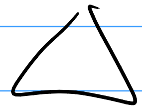
Similar to what you've seen with rings.

- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ because $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1}$
$= a \cdot a^{-1} = e$

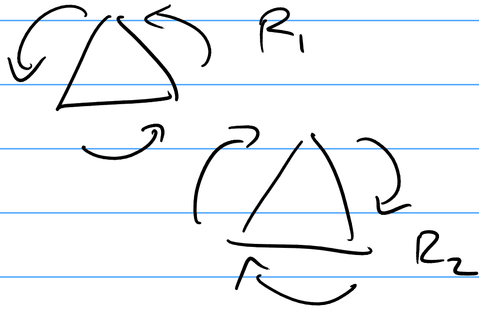
Examples:

(1) <u>Dihedral Groups</u> : symmetries of regular polygons.

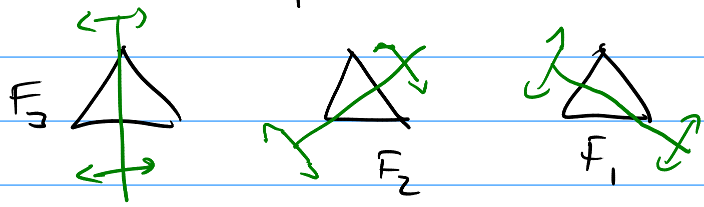
D_3 = symmetries of a triangle



$\begin{cases} e = \text{do nothing.} \\ \text{rotate by } 120° \text{ ccw} \\ \text{rotate by } 120° \text{ clockwise} \end{cases}$

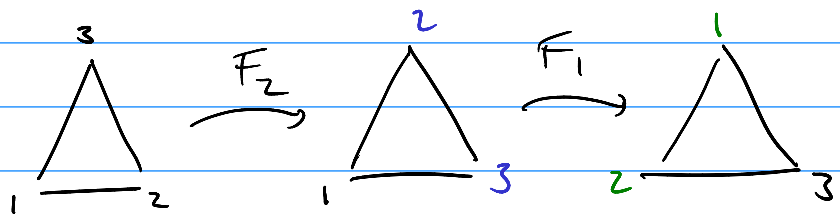


three flips:



group operation: $g \cdot h$ is "do h, then g"
like function composition.

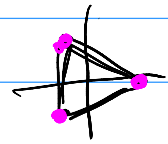
$F_1 \cdot F_2$?



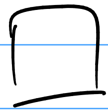
$F_1 \cdot F_2 = R_2$

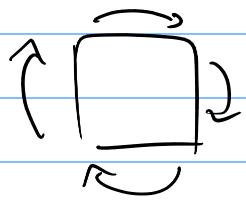
Formally, $D_3 = \{$ linear maps $\mathbb{R}^2 \to \mathbb{R}^2$ that preserve the set of three points

$(\cos 0, \sin 0)$ $(\cos 120, \sin 120)$ $\cos(240, \sin 240)$

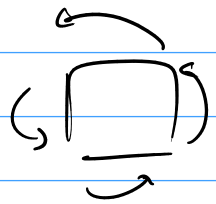


D_4 = symmetries of a square

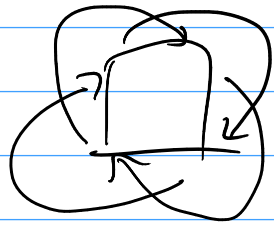
identity 

rotate 90° clockwise  R_3

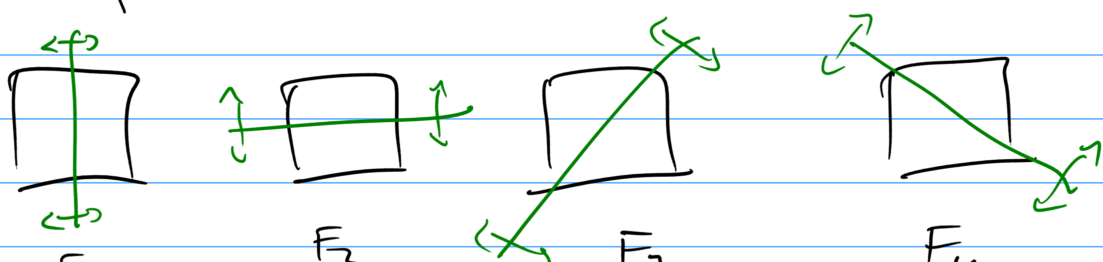
rotate 90° counterclockwise

 R_1

rotate 180°

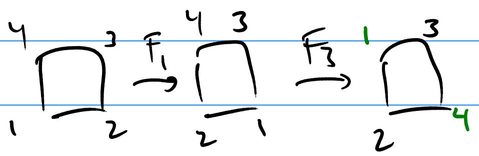
 R_2

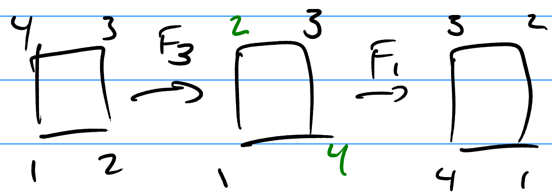
four flips



F_1 F_2 F_3 F_4

not Abelian: $F_3 \cdot F_1 = R_3$ but $F_1 \cdot F_3 = R_1$





Could check: $F_2 \cdot F_1 = F_1 \cdot F_2$

D_5: pentagon. identity, 4 rotations, 5 flips

D_6: hexagon etc.

Warning: what I call D_n some people call D_{2n}
because it has $2n$ elements.

---

2 Symmetric groups / permutation groups.

$$S_n = \left\{ \begin{array}{l} \text{all bijections from the set } \{1,2,\dots,n\} \\ \text{to itself} \end{array} \right\}$$

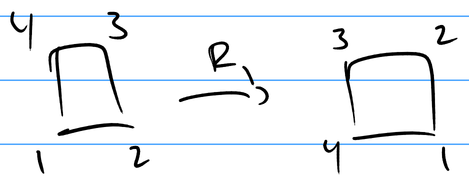
operation = composition
associative: if $r, s, t : \{1,2,..n\} \circlearrowleft$

then $(r \circ s) \circ t = r \circ (s \circ t)$

identity is the map that does nothing:
$e(m) = m$ for all $m \in \{1, 2, \dots n\}$

inverses: because they're bijections.

notice that D_4 gives a subgroup of S_4:

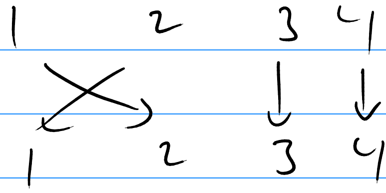


corresp to the map

$$\begin{array}{cccc} \{1, & 2, & 3, & 4\} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

$\{1, 2, 3, 4\}$

proper subgroup (not all of S_4):



doesn't come from any symmetry of the square.