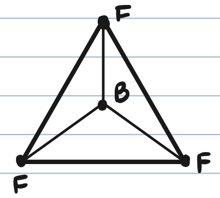
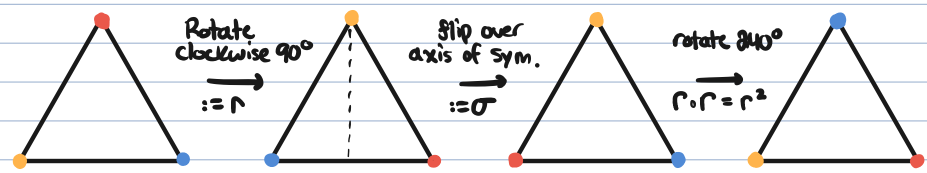
Groups

Groups are really the study of symmetries. Originally, these arise in studying symmetries of roots of polynomials.

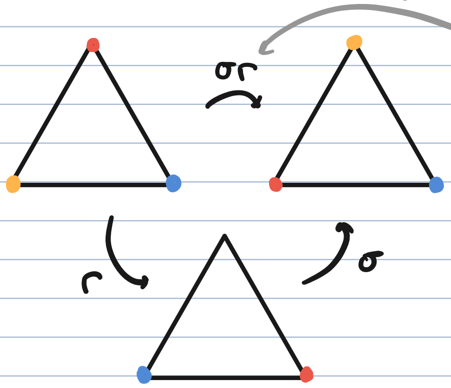
Example: Consider the molecule Boron Trifluoride BF_3:



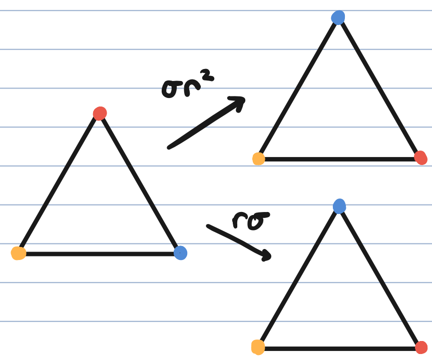
We want to describe the symmetrics of this molecule.



Note: σ^2 = identity ; everything stayed the same.

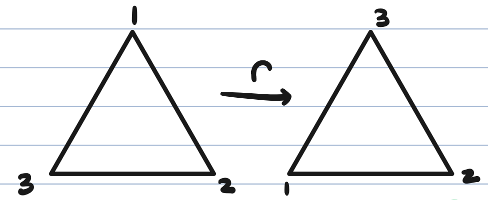


read right to left.
Like $(f\circ g)(x)$



* $\sigma r^2 = r\sigma$

The set of all symmetries $D_3 = \{id, r, r^2, \sigma, \sigma r, \sigma r^2\}$



$$r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} := (1\ 2\ 3)$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} := (1)(2\ 3) = (2\ 3)$$

$$r\sigma = (1\ 2\ 3)(2\ 3) = (1\ 2)(3) = (1\ 2)$$

$$\sigma r = (2\ 3)(1\ 2\ 3) = (1\ 3)(2) = (1\ 3)$$

The set D_3 is a group under composition. This is referred to as the <u>dihedral group in 3 elements</u>.

Given a set X, a <u>binary operation</u> on X is a function $*: X \times X \to X$.

e.g. $X = \mathbb{R}$, $* = +$, $*(a,b) = a + b$

<u>Definition:</u> Let G be a non-empty set and $*: G \times G \to G$ a binary operation. We say $(G, *)$ is a <u>group</u> if:

(i) $g_1 * g_2 \in G$, $g_1, g_2 \in G$

(ii) $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3 \quad \forall g_1, g_2, g_3 \in G$

(iii) There exists $e_G \in G$ so that $e_G * g = g = g * e_G$

(iv) $(\forall g \in G)(\exists g^{-1} \in G)$ s.t. $g * g^{-1} = e_G = g^{-1} * g$

We will write G for $(G,*)$ when $*$ is clear from context.

If $g_1 * g_2 = g_2 * g_1 \ \forall g_1, g_2 \in G$, we say G is an <u>abelian group.</u>

<u>Example</u>: 1) D_3 is a group, but not an abelian group.

2) $(\mathbb{Z}, +)$ is an abelian group.

3) $(2\mathbb{Z}, +)$ is an abelian group.
$\rightarrow 2\mathbb{Z} = \{2m \mid m \in \mathbb{Z}\}$
$e_{2\mathbb{Z}} = 0$
$-2m$ inverse

4) $(\mathbb{R}, \cdot)$ is <u>not</u> a group b/c 0 does not have an inverse.

5) $(\mathbb{R}^*, \cdot)$ is an abelian group
$\rightarrow \mathbb{R}^* = \{r \in \mathbb{R} : r \neq 0\}$.

<u>Example</u>: Let $n \in \mathbb{Z}$. Define $a \equiv b \pmod{n}$ if $n \mid (a-b)$.
This gives an equivalence relation in $\mathbb{Z}$.

For $a \in \mathbb{Z}$, $[a]_n := \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$
$= \{b \in \mathbb{Z} : n \mid (b-a)\}$
$= \{a + nk : k \in \mathbb{Z}\}$

For instance, if $n=3$:

$[1]_3 = \{1 + 3k : k \in \mathbb{Z}\}$
$= \{\dots -5, -2, 1, 4, 7, \dots\}$

For each $a \in \mathbb{Z}$, we can write: (uniquely)

$a = nq + r$ for some $q, r \in \mathbb{Z}$ w/ $0 \leq r \leq n$.

All equivalence classes are given by $[0]_n, [1]_n, \dots [n-1]_n$

Define $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
$\rightarrow \# \mathbb{Z}/n\mathbb{Z} = n.$

We can define a binary operation by

$$[a]_n + [b]_n = [a+b]_n$$ regular integer addition, then take equivalence class.

"new" addition

e.g. $n=3$

$$[2]_3 + [2]_3 = [2+2]_3 = [4]_3 = [1]_3$$ since $4 \equiv 1 \pmod 3$

<u>Well-Definedness</u>: Let $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$. WTS $[a_1]_n + [b_1]_n = [a_2]_n + [b_2]_n$.

We have $a_1 = a_2 + ns$ for some $s \in \mathbb{Z}$

and $b_1 = b_2 + nt$ for some $t \in \mathbb{Z}$

Note $[a_1]_n + [b_1]_n = [a_1 + b_1]_n$

$= [(a_2 + ns) + (b_2 + nt)]_n$

$= [(a_2 + b_2) + n(s+t)]_n$

$= [a_2]_n + [b_2]_n + \cancel{[n(s+t)]_n}$ 0 since divisible by n.

The set $\mathbb{Z}/n\mathbb{Z}$ is an abelian group.

$\rightarrow e_{\mathbb{Z}/n\mathbb{Z}} = [0]_n$

$-[a]_n = [-a]_n = [n-a]_n$