Recall: $(G, \cdot)$

cancellation law holds

$(\mathbb{Z}_n, +)$ abelian group

$U(n) := \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

" group of units in $\mathbb{Z}_n$

" inverse exists w.r.t multiplication

$U(n) = \mathbb{Z}_n^*$ (notation)

Cayley Table for $U(12)$ and $U(5)$?

$U(12) = \{1, 5, 7, 11\}$ $\qquad$ $U(5) = \{1, 2, 3, 4\}$

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Abelian group

$U(5) = \{1, 2, 3, 4\}$ Similar

also a group

In general, if p is a prime, then $U(p)$ is $\{1, 2, \ldots, p-1\}$, a group under multiplication modulo p.

Definition: If $(G, \cdot)$ is a group, the <u>order of G</u>, denoted $|G|$, is the number of elements of G

If $|G| = \infty$, $(G, \cdot)$ is said to be an <u>infinite group</u>. otherwise, $(G, \cdot)$ is a <u>finite group</u>.

<u>eg.</u> $|\mathbb{Z}_n| = n$

$|U(12)| = 4$

$|U(p)| = p-1$ for p prime

$|\mathbb{Z}| = \infty$

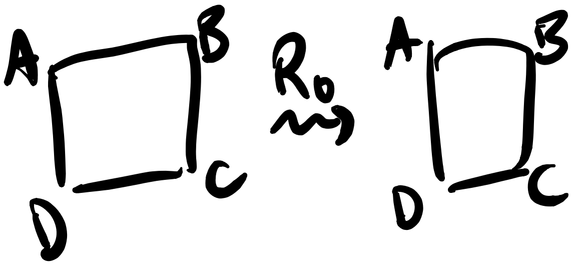
<u>Dihedral Groups</u>

D_n, $n \geq 3$

D_4, D_3

<u>symmetry</u> of a <u>polygon</u>

D_n is the set of symmetries of an regular n-gon

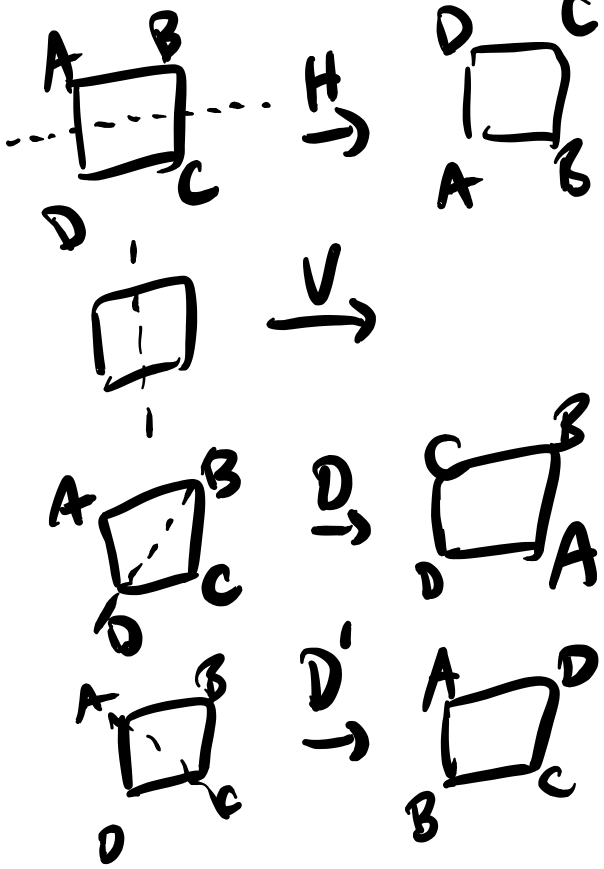


rotation by $0°$

... R_{180} ...

... R_{270} ...

$\cancel{R_{360}} = R_0$



Since $R_{270} \cdot H \neq H \cdot R_{270}$, then $(D_4, \cdot)$ is a non-abelian group (if it is a group.)

Identity for $D_4 = R_0$

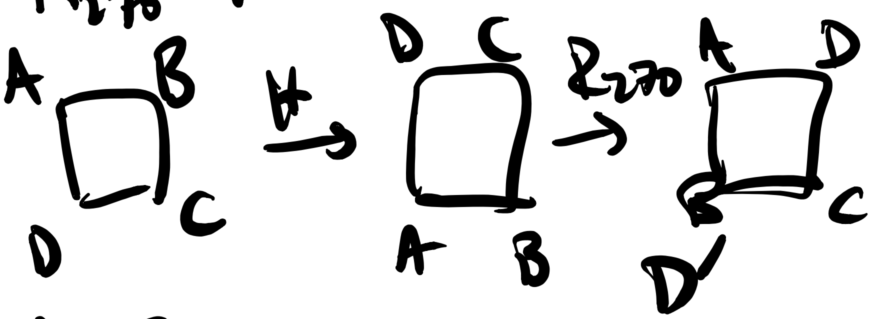
$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

Composition of Symmetries

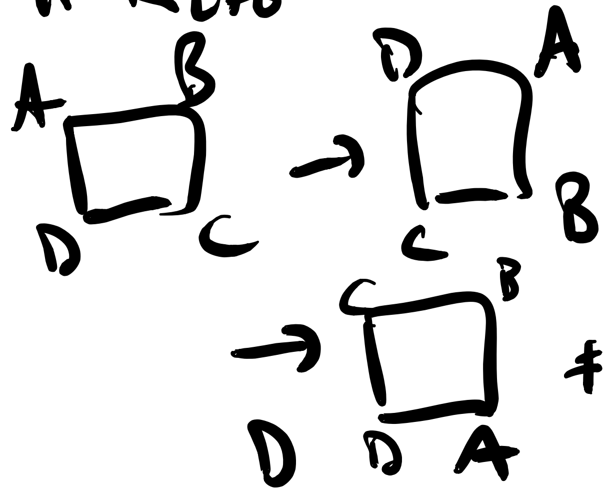
S_1 and S_2 are two symmetries

$S_1 \cdot S_2$ – apply S_2 first then apply S_1 to the result

$R_{270} \cdot H$



$H \cdot R_{270}$

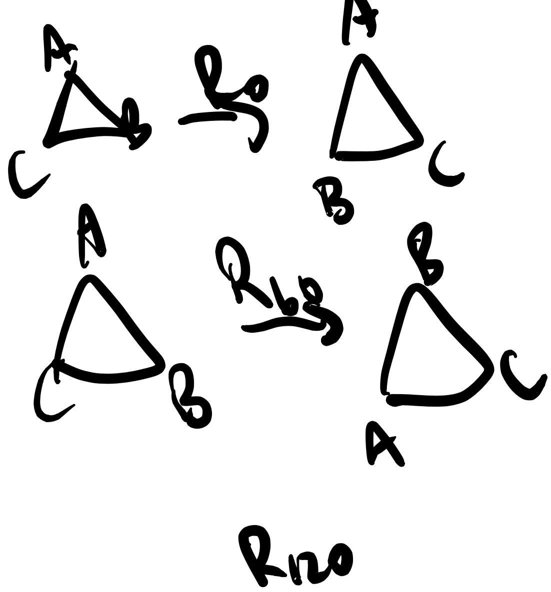


$\neq R_{270} \cdot H$

proved in lecture notes on LEARN

$|D_4| = 8$

D_3:



$|D_3| = 6$

$(D_n, \cdot)$

comp. of symmetries

is always a non-abelian group of order $2n$

proof on a/n easy to do

Symmetry group: S_3

Cayley's Theorem: any group can fit in S_n (copy inside S_n)