If R is a ring, get two groups from it:

additive group $(R, +)$.
↳ Abelian. identity is 0

group of units $(R^\times, \cdot)$
$R^\times$ is a subset of R
closed under mult: if u, v are units,
write $ux = 1$ and $vy = 1$ for some $x, y \in R$
then $uv \cdot yx = u \cdot 1 \cdot x = 1$ so uv is a unit.
and similarly on the other side.

For example, $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$

notice that $\mathbb{Z}_9^\times$ is cyclic, generated by 2:

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16 = 7$
$2^5 = 32 = 5$
$2^6 = 64 = 1$

in $\mathbb{Z}_n$ group of units is $\mathbb{Z}^\times = \{1, -1\}$

the additive group

group of units

get a group iso. $\varphi: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_9^\times$
$n \longmapsto 2^n$

bijection? just checked.
homomorphism? $\varphi(m+n) = 2^{m+n} = 2^m \cdot 2^n = \varphi(m) \cdot \varphi(n)$

$\varphi(n) = 5^n$ would also have worked.

In general, for $g \in G$, the cyclic subgroup generated by g is

$$\langle g \rangle = \{ \dots g^{-2}, g^{-1}, 1, g, g^2, \dots \} \subset G$$

if $|g| = n$ then $\langle g \rangle \cong \mathbb{Z}_n$
$g^k \longleftrightarrow k$

if $|g| = \infty$ then $\langle g \rangle \cong \mathbb{Z}$ (additive group still!)
$g^k \longleftrightarrow k$

//

CRT says $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if $\gcd(m,n) = 1$
$\uparrow$ ring iso!

look at the group of units...

$$\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$$
$\uparrow$ group iso!

$$\mathbb{Z}_{12}^\times \cong \mathbb{Z}_3^\times \times \mathbb{Z}_4^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$
$\|$ $\|$ $\|$
$\{1,5,7,11\}$ $\{1,2\}$ $\{1,3\}$
$\|$ $\|$
$\mathbb{Z}_2$ $\mathbb{Z}_2$

Proposition 2.3 in §6.2:
if $\varphi: G \to H$ is an iso. then

① $|G| = |H|$ (maybe finite or infinite)
Pf: φ is a bijection

② $\forall g \in G, \quad |g| = |\varphi(g)|$

Pf: look at $1, g, g^2, g^3, \ldots$

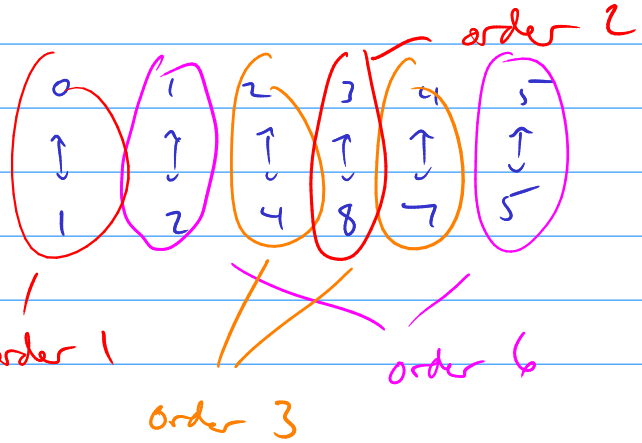
hit it with φ: $\varphi(1), \varphi(g), \varphi(g^2), \varphi(g^3), \ldots$
$= \quad 1 \quad \varphi(g) \quad \varphi(g)^2 \quad \varphi(g)^3 \ldots$

if $|g| = \infty$ then those are all distinct, and φ is injective, so those are all distinct, so $|\varphi(g)| = \infty$

if $|g| = n$ then $1, g, \ldots, g^{n-1}$ are different
but $g^n = 1$

φ injective, so $1, \varphi(g), \ldots, \varphi(g)^{n-1}$ are different
but $\varphi(g)^n = 1$

Example: $\mathbb{Z}_6$ $\quad$ $\cong$ $\quad$ $\mathbb{Z}_7^\times$



(3) if G is Abelian then H is Abelian

Pf: let $h_1, h_2 \in H$

bec. φ is surjective, can write

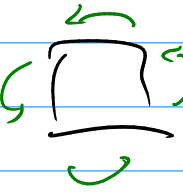
$h_1 = \varphi(g_1)$ $h_2 = \varphi(g_2)$ for some $g_1, g_2 \in G$

then $h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)$

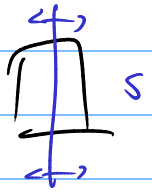
$= \varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1) = h_2 h_1$

Dihedral Groups

D_4 = symmetries of a square.

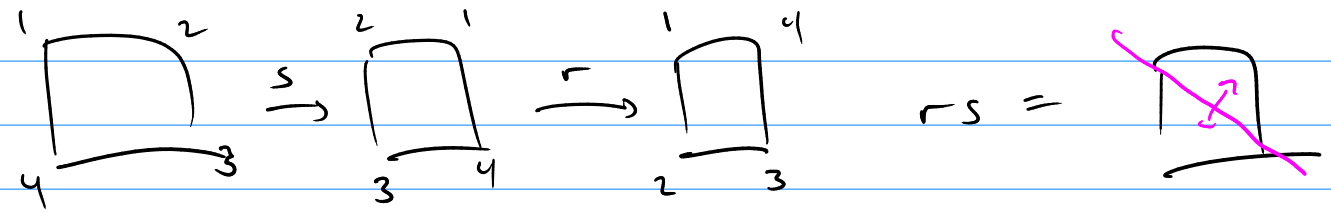
$r \in D_4$ is rotation 90° counterclockwise 

$|r| = 4$

$s \in D_4$ is reflection left-to-right 

$|s| = 2$

Notice: $rs \neq sr$



but