Review

1. G has order 35

a, b non-identity elements of different orders.

Lagrange's Thm tells us that the orders of a & b must be a divisor of 35, ie, 1, 5, 7, or 35.

Since a & b are non-identity elements, don't have order 1.

So the orders must be two of the numbers among 5, 7, and 35.

$H = \langle a, b\rangle$ is a subgroup of G, and it contains a & b, so its order must be a multiple of the order of a & of the order of b. But the only divisor of 35 that is a multiple of any pair of numbers among 5, 7, 35 is 35 itself.

So $H = G$.

$\langle a, b\rangle$ is the smallest subgroup of G that contains a & b. It's not cyclic in general. can't really describe easily as "powers of a & b" or something like that.

$\langle a\rangle$ could contain b if $|a| = 35$. Similarly $\langle b\rangle$ could contain a if $|b| = 35$.

2. $\alpha = \underbrace{(1\,3)}_{\text{odd}}\underbrace{(3\ 4\ 7)}_{\text{even}}\underbrace{(2\ 4\ 3)}_{\text{even}}\underbrace{(1\,2)}_{\text{odd}}$ is even!

even/odd permutations multiply the same way as even/odd numbers add.

You could write α in disjoint cycle form first, but that's unnecessary work in this case.

$\alpha = (1\ 7)(2\ 3)(4) = \underbrace{(1\,7)\,(2\,3)}_{2\ \text{2-cycles}}$ is even.

[If it was $\beta = (1\,3)(3\,4\,7)(3\,4\,7)$, then:

$\beta = (1\ 3\ 7\ 4)$]

odd, b/c is a cycle of even length.

3. $\mathbb{Z}_{20}$ cyclic group $= \langle 1 \rangle$

Has a unique subgroup of every order dividing 20.

In particular, has a unique subgroup of order 4.

$\langle 5 \rangle = \{0, 5, 10, 15\}$ has order 4, so 5 is a generator.

Any number $k = 0, \ldots, 19$ such that $\gcd(k, 20) = 5$, will also be a generator for the same subgroup.

That only happens for $k = 5$ & 15.

$\langle 15 \rangle = \{0, 15, 10, 5\} = \langle 5 \rangle$.

$2 \cdot 15 = 30$ mod 20 $= 10$

$3 \cdot 15 = 45$ mod 20 $= 5$

4. $\langle R_{90} \rangle$ in D_4.

How many cosets? 2.

R_{90} has order 4, so $\langle R_{90} \rangle$ has order 4,

D_4 has order 8, so # of cosets is $8/4 = 2$

$\langle R_{90} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\}$

other coset = everything else, ie, all reflections!

Recall: cosets of H partition G into pieces of equal sizes.

5. $9^{603} \bmod 7$

$= 2^{603} \bmod 7$

$= (2^6)^{100} 2^3 \bmod 7$

$= 2^3 \bmod 7$

$= 1.$

$9 \bmod 7 = 2.$

① $a^p \bmod p = a$

② $a^{p-1} \bmod p = 1$ if $\gcd(a,p) = 1.$

$2^6 \bmod 7 = 1.$ (FLT)

$ab \bmod n = (a \bmod n)(b \bmod n) \bmod n.$

Consider $U(p)$. It's a group of $p-1$ elements so any element $a \in U(p)$ has order dividing $p-1$ by Lagrange. So $a^{p-1} = 1$. ◻

2^{603}
$= 2^{86 \cdot 7 + 1}$
$= (2^7)^{86} \cdot 2$
$= 2^{86} \cdot 2$
$= 2^{12 \cdot 7 + 2} \cdot 2$
$= (2^7)^{12} \cdot 2^2 \cdot 2$
$= 2^{12} \cdot 2^2 \cdot 2$
$= 2^7 \cdot 2^5 \cdot 2^2 \cdot 2$
$= 2^5 \cdot 2^2 \cdot 2^2$
$= 2 \cdot 2^2$
$= 2^3$
$= 1.$

$U(10) = \{1, 3, 7, 9\}$

$T_3 : U(10) \longrightarrow U(10)$

$x \longmapsto 3x \; [\bmod 10]$

not an isomorphism (not operation-preserving) but it is bijective, ie, it is a permutation.

So I can write T_3 in disjoint cycle form.

$T_3 = (1 \; 3 \; 9 \; 7)$

$U(8) = \{1, 3, 5, 7\}$
$U(12) = \{1, 5, 7, 11\}.$

Consider $\varphi : U(8) \to U(12)$ where:

$\varphi(1) = 1$
$\varphi(3) = 5$
$\varphi(5) = 7$
$\varphi(7) = 11.$

$\longleftrightarrow$

1	1
3	5
5	7
7	11

we want to now show that φ is an isomorphism.

It's clear that it's bijective. To show that it's operation preserving...

we have to show that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in U(8)$.
16 cases

- if $a=b$, then $a^2=1$, because every element has order dividing 2.

  so $\varphi(ab) = \varphi(a^2) = \varphi(1) = 1$

  4/16 cases

  on the other hand, $\varphi(a)\varphi(b) = \varphi(a)^2$ but every element of $U(12)$ has order 2,

  so $\varphi(a)^2 = 1$, so $\varphi(a)\varphi(b) = \varphi(a)^2 = 1$.

  so we have $\varphi(a)\varphi(b) = \varphi(ab)$.

- if $a=1$ & b is anything... $\varphi(ab) = \varphi(b)$ & $\varphi(a)\varphi(b) = 1 \cdot \varphi(b) = \varphi(b)$.

  6/16 cases

  so again we have $\varphi(ab) = \varphi(a)\varphi(b)$.

  Same argument if a is anything & $b=1$.

- if $a=3$ & $b=5$, $\varphi(ab) = \varphi(7) = 11$

  2/16 cases

  $\varphi(a)\varphi(b) = 5 \cdot 7 = 11$

  Same for $a=5$ & $b=3$.

- ...