① • $\langle \mathbb{Z}_1^*, \cdot \rangle = \{\}$

• $U_1 = \{\}$

• $\langle \mathbb{Z}_{11}^*, \cdot \rangle = \{[1], [2], \dots, [10]\}$

• $\langle \mathbb{Z}_{21}^*, \cdot \rangle = \{[1], [2], \dots, [20]\}$

② • $\phi(81) = 81 \cdot (1 - 1/3) = 54$

• $\phi(281) = 281 - 1 = 280$

• $\phi(3817) = (11-1)(347-1) = 3460$

• $\phi(4811) = (17-1)(283-1) = 4560$

③ • $\langle \mathbb{Z}_{19}, + \rangle = \{[0], [1], \dots, [18]\}$

$|[0]| = 1 \quad , \quad |[1]| = \dots = |[18]| = 19$

Since 19 is prime, all elements in $\langle \mathbb{Z}_{19}, + \rangle$ are coprime with 19. thus, in order for

$$n \cdot g \mod 19 = 0 \quad , \quad n \in \mathbb{N} \quad \text{and} \quad g \in \langle \mathbb{Z}_{19}, + \rangle$$

to hold (which is what a generator is in the case of a residue class) n must be 19! ~~Therefore~~
Therefore, all ranks of elements in $\langle \mathbb{Z}_{19}, + \rangle$ are 19 (except [0]).

• $\langle \mathbb{Z}_{29}^*, \cdot \rangle = \{[1], \dots, [28]\}$

$|[1]| = 1 \quad , \quad |[2]| = \dots = |[28]| = \infty$

Same argument here, but

$$g^n \mod 29 = 1 \quad , \quad n \in \mathbb{N} \quad \text{and} \quad g \in \langle \mathbb{Z}_{29}, \cdot \rangle$$

since all elements are coprime with 29, there exists no element n s.t. the above holds for any g (except 1).

④ • $H = \{[1], [2], [4]\}$

Is indeed a subset of $U_9 = \{[1], [2], [4], [5], [7], [8]\}$

H is not a group.

(4)

* all elements in H are residue classes, and for residue classes $[a],[b]$:

$$[a]\cdot[b] = [a\cdot b] = [ab] \sim \quad a\cdot b = ab$$

thus:

$$(a\cdot b)\cdot c = ab\cdot c = abc$$

$$a\cdot(b\cdot c) = a\cdot bc = abc$$

for all $a,b,c \in H$

* if we take $e=[1]$, then

$$[a]\cdot[1] = [a]$$

$$[1]\cdot[a] = [a]$$

for all $[a] \in H$

* Now, for ~~element~~ $[4]$, there exists no ~~....~~ element $a' \in H$ s.t.

$$[4]\cdot a' = e = [1]$$

~~Therefore~~ There fore, H is not a group. Also ~~a~~ making it not a subgroup.

$$H = \{[1],[2],[5]\}$$

is also a subset of U_9

is ~~also~~ not a group

* ~~...~~ same argument as in previous point

* same argument as in previous point

* and for each $a \in H$, there exists an element s.t.

$$a\cdot a' = e = a'\cdot a$$

for $[1]$: $[1]\cdot[1] = [1]$

for $[2]$: $[2]\cdot\underline{[5]} = [1]$, $\underline{[5]}\cdot[2] = [1]$

for $[5]$: $[5]\cdot\underline{[2]} = [1]$, $\underline{[2]}\cdot[5] = [1]$

* For $[2]\cdot[2] = [4]$, but $[4] \notin H$

(4) ~~[illegible]~~

Since H is ~~both~~ a subset of U_9 ~~and~~ but not a group, it is ~~indeed~~ not a subgroup of U_9

- $H = \{[1], [2], [4], [8]\}$

  is indeed a subset of U_9

  is not a group since there is no element $a' \in H$ s.t. $[4] \cdot a' = [1]$

  $\Rightarrow$ not a subgroup

- $H = \{[1], [4], [7], [8]\}$

  is a subset of U_9

  is not a group since there is no element $a' \in H$ s.t. $[8] \cdot a' = [1]$

  $\Rightarrow$ not a subgroup

- $H = \{[1], [4], [5], [7], [8]\}$

  is a subset of U_9

  is not a group since there is no element $a' \in H$ s.t. $[8] \cdot a' = [1]$

(5) 2 subgroup ~~[illegible]~~ $\langle 1 \rangle$ of $\mathbb{Z}_{41}$

$\langle 1 \rangle = \{[1], \dots, [40]\}$

1 a. Generators of $\mathbb{Z}_{11}$: $[1], \dots, [10]$

b. In the case that p is prime ~~[illegible]~~ all elements in $\mathbb{Z}_p$ are generators for the group

~~There are two cases to consider:~~

~~1. an element in $\mathbb{Z}_p$ is odd~~
~~2. an element in $\mathbb{Z}_p$ is even.~~

~~(1) in the case that an element $g \in \mathbb{Z}_p$ is odd, multiplying g by an $n \in \mathbb{N}$ s.t.~~

~~$1 \cdot g \bmod p = g$~~

~~[illegible]~~

~~$0 \cdot g \bmod p = 0$~~

⑤ 3. None of the elements in $\langle 3 \rangle$ are generators for $\mathbb{Z}_{27}$ since for an element $q \in \langle 3 \rangle$ $q = n \cdot 3$, $n \in \mathbb{N}$. And thus

$$\gcd(n \cdot 3, 27) = \gcd(n \cdot 3, 9 \cdot 3) = 3 \neq 1$$

Meaning that for any q

$$n \cdot q \mod 27 = 0$$

⑥ Since '$\cdot$' is commutative, G is an abelian group. Therefore the left cosets will coincide with the right ones (and vice versa):

$$U_{28} = \{[1], [3], [5], [9], [11], [13], [15]$$
$$[17], [23], [25], [27]\}$$

$$[1]H = \{[1], [9], [25]\}$$

$$3H = \{3, 27, 75\}$$

$$\vdots$$

$$27H = \{27, 243, 675\}$$

⑦ · $\langle \mathbb{Z}_6, + \rangle$ and $\langle U_{14}, \cdot \rangle$ with $\varphi(a) = 3^a$

$[a],[b] \in \mathbb{Z}_6$: $\varphi([a]+[b]) = 3^{[a]+[b]} = 3^{[a+b]}$

$\varphi([a]) \cdot \varphi([b]) = 3^{[a]} \cdot 3^{[b]} = 3^{[a]+[b]} = 3^{[a+b]}$

$\Rightarrow$ Yes, the groups are a homomorphism with φ (epimorphism)

· $\langle \mathbb{Z}, + \rangle$ and $G = \{1, -1\}$ with $\varphi(a) \begin{cases} 1 & \text{if } a \text{ is even} \\ -1 & \text{if } a \text{ is odd} \end{cases}$

G is not a group, (we're missing an operator), therefore there can be no homomorphism.

· $\langle \mathbb{R}^*, \cdot \rangle$ with $\varphi(a) = a^2$

$a, b \in \mathbb{R}^*$: $\varphi(a \cdot b) = (a \cdot b)^2 = a^2 \cdot b^2$

$\varphi(a) \cdot \varphi(b) = a^2 \cdot b^2$

$\Rightarrow$ Yes, the groups are a homomorphism with φ it's an endomorphism since it maps to the same group.

⑦ · $\langle \mathbb{Z}_7^*, \cdot \rangle$ with $\varphi(a) = a$

$a, b \in \mathbb{Z}_7^*$: $\varphi(a \cdot b) = a \cdot b$

$\varphi(a) \cdot \varphi(b) = a \cdot b$

⇒ the group is homomorphic with φ. It is also automorphic since it maps onto itself and the mapping is bijective.

· $\langle \mathbb{Z}, + \rangle$ with $\varphi(a) = 2a$

$a, b \in \mathbb{Z}$: $\varphi(a \cdot b) = 2(a \cdot b) = 2 \cdot a \cdot b$

$\varphi(a) \cdot \varphi(b) = (2a) \cdot (2b) = 4 \cdot a \cdot b$

⇒ the group in not homomorphic with φ

⑧ · $\mathbb{F}_{2^3} =$