HW #3

① (a)

homomorphism: Let $x, y \in \mathbb{Z}$. Then

$\varphi(x+y) = 5(x+y) = 5x+5y = \varphi(x)+\varphi(y)$.
So φ is a homomorphism.

1-1: Suppose $\varphi(x) = \varphi(y)$ where $x, y \in \mathbb{Z}$.
Then $5x = 5y$. So $x = y$. So φ is 1-1.

onto: φ is not onto. For example, $1 \in \mathbb{Z}$, but there does not exist $x \in \mathbb{Z}$ with $\varphi(x) = 1$.

(b)

φ is not a homomorphism For example,

$\varphi(2+3) = \varphi(5) = 2(5)-1 = 9$

but $\varphi(2)+\varphi(3) = [2(2)-1]+[2(3)-1] = 3+5 = 8$.

φ is 1-1: Suppose $\varphi(x) = \varphi(y)$ where $x, y \in \mathbb{Z}$.
Then, $2x-1 = 2y-1$. So, $x = y$.

φ is not onto: $0 \in \mathbb{Z}$ but $2x-1 \neq 0$ for all $x \in \mathbb{Z}$.

(c)

φ is a hom: Let $x, y \in \mathbb{Q}$. Then

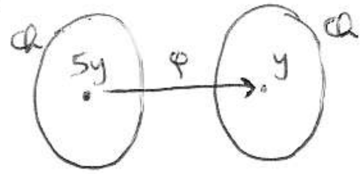
$\varphi(x+y) = \frac{x+y}{5} = \frac{x}{5} + \frac{y}{5} = \varphi(x) + \varphi(y)$.

φ is 1-1: Suppose $\varphi(x) = \varphi(y)$ where $x, y \in \mathbb{Q}$.

Then $\frac{x}{5} = \frac{y}{5}$. So, $x = y$.

φ is onto: Let $y \in \mathbb{Q}$. Then $5y \in \mathbb{Q}$ and

$\varphi(5y) = \frac{5y}{5} = y$.



Therefore φ is an isomorphism.

(d) φ is a hom: Let $x, y \in \mathbb{Q}^*$. Then

$\varphi(xy) = (xy)^2 = x^2 y^2 = \varphi(x)\varphi(y)$.

φ is not 1-1: $\varphi(1) = 1^2 = 1 = (-1)^2 = \varphi(-1)$.

φ is not onto: $2 \in \mathbb{Q}$, but there is no $x \in \mathbb{Q}^*$ with $\varphi(x) = x^2 = 2$, since $\pm\sqrt{2}$ are not rational.

(e)

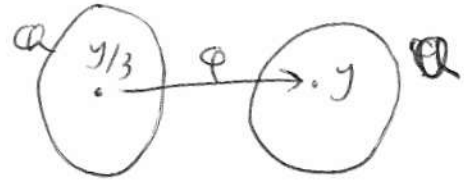
φ is not a homomorphism:

$$\varphi(2 \cdot 5) = 3(2 \cdot 5) = 30$$

$$\varphi(2)\varphi(5) = [3 \cdot 2][3 \cdot 5] = 90$$

φ is 1-1 Suppose $\varphi(x) = \varphi(y)$ where $x, y \in \mathbb{Q}^*$. Then $3x = 3y$. So, $x = y$.

φ is onto: Suppose $y \in \mathbb{Q}^*$. Then $y/3 \in \mathbb{Q}^*$ and $\varphi\left(\frac{y}{3}\right) = 3\left(\frac{y}{3}\right) = y$.



(f) φ is a hom: Let $x, y \in \mathbb{R}$. Then

$$\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y).$$

φ is 1-1: Suppose $\varphi(x) = \varphi(y)$ where $x, y \in \mathbb{R}$. Then $e^x = e^y$. Thus, $\ln(e^x) = \ln(e^y)$. So, $x = y$.

φ is not onto $-1 \in \mathbb{R}^*$ but there is no $x \in \mathbb{R}$ with $\varphi(x) = e^x = -1$.

(2)

(a)

closure: Let $x, y \in n\mathbb{Z}$. Then $x = nk_1$ and $y = nk_2$ where $k_1, k_2 \in \mathbb{Z}$. So, $x + y = n(k_1 + k_2) \in n\mathbb{Z}$ since $k_1 + k_2 \in \mathbb{Z}$.

associativity: $n\mathbb{Z} \subseteq \mathbb{Z}$ and $\mathbb{Z}$ is associative, so $n\mathbb{Z}$ is associative.

identity: $0 = n(0) \in n\mathbb{Z}$.

inverses: Let $x \in n\mathbb{Z}$. Then $x = nk$ where $k \in \mathbb{Z}$. Then $-x = n(-k) \in n\mathbb{Z}$ and

$$x + (-x) = nk + n(-k) = 0$$

and $(-x) + x = n(-k) + nk = 0$.

So the inverse of x is in $n\mathbb{Z}$.

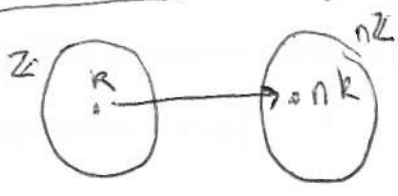
(b) Let $\varphi : \mathbb{Z} \to n\mathbb{Z}$ be defined by $\varphi(x) = nx$.

φ is a hom: Let $x, y \in \mathbb{Z}$. Then $\varphi(x+y) = n(x+y) = nx + ny = \varphi(x) + \varphi(y)$.

φ is 1-1: Suppose $\varphi(x) = \varphi(y)$ where $x, y \in \mathbb{Z}$. Then $nx = ny$.

So, $x = y$.

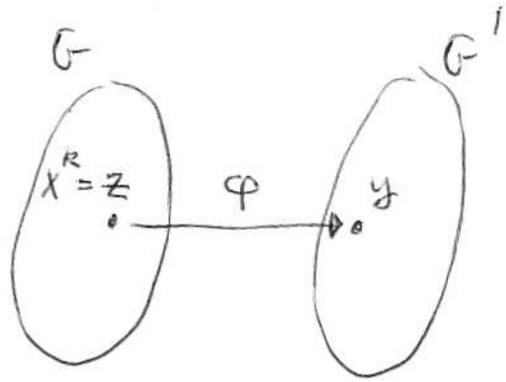
φ is onto: Let $y \in n\mathbb{Z}$. Then $y = nk$ where $k \in \mathbb{Z}$. And $\varphi(k) = nk = y$.



Thus, φ is an isomorphism and $n\mathbb{Z} \cong \mathbb{Z}$.

(3) Since G is cyclic, $G = \langle x \rangle$ ~~where~~ where $x \in G$.

<u>Claim: $G' = \langle \varphi(x) \rangle$</u>: Since $\varphi(x) \in G'$ we know that ~~so~~ $\langle \varphi(x) \rangle \subseteq G'$. Now let's show that $G' \subseteq \langle \varphi(x) \rangle$. Let $y \in G'$. Since φ is onto there exists $z \in G$ with $\varphi(z) = y$.



Since $z \in G$ and $G = \langle x \rangle$, there exists $k \in \mathbb{Z}$ with $z = x^k$. Then,

$$y = \varphi(z) = \varphi(x^k) \underset{\boxed{\text{since } \varphi \text{ is a hom.}}}{=} [\varphi(x)]^k \in \langle \varphi(x) \rangle.$$

Therefore, $G' = \langle \varphi(x) \rangle$.

(4) $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$

$\langle r \rangle = \{1, r, r^2, \dots, r^{n-1}\}$ is cyclic of size n. By the classification theorem of cyclic groups, $\langle r \rangle \cong \mathbb{Z}_n$ and $\varphi(r^k) = \overline{k}$ is an isomorphism.

(5)

We need a lemma:

Lemma: Let G' be a group and $x \in G'$. Suppose that x has order n. If $x^k = e$ for some integer k, then n divide k.

proof: By the division algorithm

$$k = qn + r \text{ where } 0 \leq r < n$$

for some $q, r \in \mathbb{Z}$.

Also,

$$e = x^k = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r.$$

Since $0 \leq r < n$ and x has order n and $x^r = e$ we must have that $r = 0$. Thus, $k = qn$. So, n divides k. ∎

(a) Let k be the order of x. Then $x^k = e$ where e is the identity of G. Since φ is a homomorphism $\varphi(e) = e'$ where e' is the identity of G' and

$$[\varphi(x)]^k = \varphi(x^k) = \varphi(e) = e'.$$

By the lemma, k divides the order of $\varphi(x)$.

(5) (b) Let n be the order of x and m be the order of $\varphi(x)$.

By (a) we know that $m \leq n$.

Note that $\varphi(x^m) = [\varphi(x)]^m = e'$.

$\boxed{m = \text{order}(\varphi(x))}$

Since φ is 1-1 and $\varphi(x^m) = e' = \varphi(e)$ we must have that $x^m = e$. By the lemma, this shows that n divides m. So, $n \leq m$.

Since $n \leq m$ and $m \leq n$ we must have that $n = m$.