Prop: (Homomorphisms out of cyclic groups)
Let $G = \langle x \rangle$ be a cyclic group where $x \in G$. Let H be another group.

<u>case 1: Suppose x has order n.</u>

Let $y \in H$ with $\text{order}(y) = m$. If m divides n, then the map $\varphi : G \to H$ given by $\varphi(x^i) = y^i$ is a homomorphism. Furthermore, any homomorphism $\psi : G \to H$ must be of this form. [That is, there is a $y \in H$ with $\text{order}(y)$ dividing n and $\psi(x^i) = y^i$].

<u>case 2: Suppose x has infinite order.</u>

Let $y \in H$. Define $\varphi : G \to H$ by $\varphi(x^i) = y^i$.
Then, φ is a homomorphism. Furthermore, any homomorphism $\psi : G \to H$ is gotten in this way.

proof:

<u>case 1:</u> Suppose $y \in H$ with $\text{order}(y) = m$. Suppose m divides n. Then, $n = mk$ for some integer k.
Let $\varphi : G \to H$ be defined by $\varphi(x^i) = y^i$.
We first show that φ is well-defined.
Suppose $x^a = x^b$ where $a \geq b$. Then $x^{a-b} = 1_G$.
By the lemma, $a - b = qn$ for some $q \in \mathbb{Z}$.

Note that

$$y^{a-b} = \varphi\left(x^{a-b}\right) = \varphi\left(x^{nq}\right) = \varphi\left(x^{mkq}\right)$$
$$= y^{mkq} = (y^m)^{kq} = 1_H^{kq} = 1_H.$$

So, again by the lemma, $a-b = m\ell$ for some $m \in \mathbb{Z}$. So, $\varphi(x^a) = y^a = y^{b+m\ell} = y^b y^{m\ell} = y^b 1_H = y^b = \varphi(x^b)$.

Now we show that φ is a homomorphism. Let $w, z \in G$. Then, $w = x^c$ and $z = x^d$ for some $c, d \in \mathbb{Z}$. So, $\varphi(wz) = \varphi(x^c x^d) = \varphi(x^{c+d}) = y^{c+d} = y^c y^d = \varphi(x^c)\varphi(x^d) = \varphi(w)\varphi(z)$.

Now suppose $\psi : G \to H$ is a homomorphism. Let $y = \psi(x)$. By induction and the fact that ψ is a homomorphism one can show that $\psi(x^i) = y^i$ for all integers i. Let $m = \text{order}(y)$. By the division algorithm $n = mq + r$ with $0 \le r < m$ for some $q, r \in \mathbb{Z}$. Thus,

$$1_H = \varphi(x^n) = \varphi\left(x^{mq+r}\right) = y^{mq+r} = (y^m)^q y^r$$
$$= 1_H^q y^r = y^r.$$

Since $y^r = 1$ and $0 \le r < m$ we must have $r = 0$. Thus, $n = mq$. So, m divides n.

case 2: Exercise. (This is similar to part 1 but is easier since there is no well-defined part and no order stuff.)

$\blacksquare$