Isomorphisms & cyclic groups

Theorem: Let $G = \langle a \rangle$.

1.) If $|a| = n < \infty$, then $|G| = n$, and $G = \{e, a, a^2, a^3, \dots, a^{n-1}\}$

2.) If $|a| = \infty$, then $|G| = \infty$ and $a^x \neq a^y \quad \forall\ x \neq y$ in $\mathbb{Z}$.

Pf:

1.) Suppose $|a| = n < \infty$. Then, by a HW problem $a^i \neq a^j \ \forall$ $i, j \in \{0, \dots, n-1\}$.

Consider $a^m \in G$, some $m \in \mathbb{Z}$. Then we can write

$m = nx + i$ for some $x \in \mathbb{Z}$, $i \in \{0, \dots, n-1\}$.

Thus, $a^m = a^{nx+i} = (a^n)^x a^i = e \cdot a^i$, so $a^m \in \{e, a, a^2, \dots, a^{n-1}\}$.

$\Rightarrow G = \{e, a, \dots, a^{n-1}\}$, as desired.

2.) Assume $|a| = \infty$. Then $a^i \neq e \quad \forall \ i \in \mathbb{Z}_+$.

Let $x, y \in \mathbb{Z}$ s.t. $x \neq y$. WLOG assume $x < y$.

Then if $a^x = a^y \Rightarrow a^y a^{-x} = e \Rightarrow a^{y-x} = e$, a contradiction.

Thus, $a^x \neq a^y$, so $|G| = \infty$. □

Theorem: If G is a finite cyclic group of order n, generated by a then $G \cong \mathbb{Z}_n$.

Proof: Define $f : \mathbb{Z}_n \to G$ by $f(x) = a^x$.

If $x, y \in \mathbb{Z}_n$, then $f(x +_n y) = a^{x+_n y} = a^x a^y$, since $a^{x+_n y} = a^{x+y}$.

Suppose $f(x) = f(y)$. Then $a^x = a^y$. Since $x, y \in \mathbb{Z}_n$, $x = y$ by Hw problem, so f is injective.

Let $b \in G$. Then $b = a^i$, some $i \in \{0, \ldots, n-1\}$, so $f(i) = b$, so f is surjective, and thus an isomorphism.

Theorem: If $G = \langle a \rangle$ and a has infinite order, then $G \cong \mathbb{Z}$.

Proof: Define $f: \mathbb{Z} \to G$ by $f(x) = a^x$.

Then $f(x+y) = a^{x+y} = a^x a^y = f(x) f(y)$, so f is a homomorphism.

Suppose $f(x) = f(y)$. Then $a^x = a^y \implies x = y$ by previous theorem, so f is injective.

Let $b \in \langle a \rangle$. Then $b = a^i$, some $i \in \mathbb{Z}$. So $f(i) = b$, so f is surjective. $\square$

Cor: Every infinite cyclic group is countable.

Ex: $\mathbb{R}$ is not cyclic.

Not all countable groups are cyclic:

Ex: $\langle \mathbb{Q}, + \rangle$ is not cyclic. Suppose $\mathbb{Q}$ is cyclic. Then

$\exists \; x \neq 0 \in \mathbb{Q}$ s.t. $\forall \; y \in \mathbb{Q}$, $y = nx$ for some $n \in \mathbb{Z}$.

But $\frac{x}{2} \neq nx$ for $n \in \mathbb{Z}$, so $\mathbb{Q}$ is not cyclic.

Ex: $\mathbb{Z} \times \mathbb{Z}$ is not cyclic (HW)

Ex: D_{2n} is never abelian, so it's never cyclic.
$n > 2$