proof that all subgroups of a cyclic group are cyclic

Canonical name	ProofThatAllSubgroupsOfACyclicGroupAreCyclic
Date of creation	2013-03-22 13:30:47
Last modified on	2013-03-22 13:30:47
Owner	Wkbj79 (1863)
Last modified by	Wkbj79 (1863)
Numerical id	10
Author	Wkbj79 (1863)
Entry type	Proof
Classification	msc 20A05
Related topic	ProofThatEverySubringOfACyclicRingIsACyclicRing

The following is a proof that all subgroups of a cyclic group are cyclic.

Proof. Let G be a cyclic group and $H \leq G$. If G is trivial, then $H = G$, and H is cyclic. If H is the trivial subgroup, then $H = \{e_G\} = \langle e_G \rangle$, and H is cyclic. Thus, for the of the proof, it will be assumed that both G and H are nontrivial.

Let g be a generator of G. Let n be the smallest positive integer such that $g^n \in H$.

Claim: $H = \langle g^n \rangle$

Let $a \in \langle g^n \rangle$. Then there exists $z \in \mathbb{Z}$ with $a = (g^n)^z$. Since $g^n \in H$, we have that $(g^n)^z \in H$. Thus, $a \in H$. Hence, $\langle g^n \rangle \subseteq H$.

Let $h \in H$. Then $h \in G$. Let $x \in \mathbb{Z}$ with $h = g^x$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $x = qn + r$. Thus, $h = g^x = g^{qn+r} = g^{qn}g^r = (g^n)^q g^r$. Therefore, $g^r = h(g^n)^{-q}$. Recall that $h, g^n \in H$. Hence, $g^r \in H$. By choice of n, r cannot be positive. Thus, $r = 0$. Therefore, $h = (g^n)^q g^0 = (g^n)^q e_G = (g^n)^q \in \langle g^n \rangle$. Hence, $H \subseteq \langle g^n \rangle$.

This proves the claim. It follows that every subgroup of G is cyclic. $\square$