generator

Canonical name	Generator
Date of creation	2013-03-22 13:30:39
Last modified on	2013-03-22 13:30:39
Owner	Wkbj79 (1863)
Last modified by	Wkbj79 (1863)
Numerical id	10
Author	Wkbj79 (1863)
Entry type	Definition
Classification	msc 20A05
Related topic	GeneratingSetOfAGroup
Related topic	ProperGeneratorTheorem

If G is a cyclic group and $g \in G$, then g is a *generator* of G if $\langle g \rangle = G$.

All infinite cyclic groups have exactly 2 generators. To see this, let G be an infinite cyclic group and g be a generator of G. Let $z \in \mathbb{Z}$ such that g^z is a generator of G. Then $\langle g^z \rangle = G$. Then $g \in G = \langle g^z \rangle$. Thus, there exists $n \in \mathbb{Z}$ with $g = (g^z)^n = g^{nz}$. Therefore, $g^{nz-1} = e_G$. Since G is infinite and $|g| = |\langle g \rangle| = |G|$ must be infinity, $nz - 1 = 0$. Since $nz = 1$ and n and z are integers, either $n = z = 1$ or $n = z = -1$. It follows that the only generators of G are g and g^{-1}.

A finite cyclic group of order n has exactly $\varphi(n)$ generators, where φ is the Euler totient function. To see this, let G be a finite cyclic group of order n and g be a generator of G. Then $|g| = |\langle g \rangle| = |G| = n$. Let $z \in \mathbb{Z}$ such that g^z is a generator of G. By the division algorithm, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $z = qn + r$. Thus, $g^z = g^{qn+r} = g^{qn}g^r = (g^n)^q g^r = (e_G)^q g^r = e_G g^r = g^r$. Since g^r is a generator of G, it must be the case that $\langle g^r \rangle = G$. Thus, $n = |G| = |\langle g^r \rangle| = |g^r| = \dfrac{|g|}{\gcd(r, |g|)} = \dfrac{n}{\gcd(r, n)}$. Therefore, $\gcd(r, n) = 1$, and the result follows.