automorphism group of a cyclic group

Canonical name	AutomorphismGroupOfACyclicGroup
Date of creation	2013-03-22 18:42:35
Last modified on	2013-03-22 18:42:35
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	6
Author	rm50 (10146)
Entry type	Theorem
Classification	msc 20A05
Classification	msc 20F28

Theorem 1. *The automorphism group of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, which is of order $\phi(n)$ (here ϕ is the Euler totient function).*

Proof. Choose a generator x for $\mathbb{Z}/n\mathbb{Z}$. If $\rho \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, then $\rho(x) = x^a$ for some integer a (defined up to multiples of n); further, since x generates $\mathbb{Z}/n\mathbb{Z}$, it is clear that a uniquely determines ρ. Write ρ_a for this automorphism. Since ρ_a is an automorphism, x^a is also a generator, and thus a and n are relatively prime[1]. Clearly, then, every a relatively prime to n induces an automorphism. We can therefore define a surjective map

$$\Phi : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times : \rho_a \mapsto a \pmod{n}$$

Φ is also obviously injective, so all that remains is to show that it is a group homomorphism. But for every $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have

$$(\rho_a \circ \rho_b)(x) = \rho_a(x^b) = (x^b)^a = x^{ab} = \rho_{ab}(x)$$

and thus

$$\Phi(\rho_a \circ \rho_b) = \Phi(\rho_{ab}) = ab \pmod{n} = \Phi(\rho_a)\Phi(\rho_b)$$

□

References

[1] Dummit, D., Foote, R.M., *Abstract Algebra, Third Edition*, Wiley, 2004.

[1]If they were not, say $(a, n) = d$, then $(x^a)^{n/d} = (x^{a/d})^n = 1$ so that x^a would not generate.