criterion for cyclic rings to be principal ideal rings

Canonical name	CriterionForCyclicRingsToBePrincipalIdealRings
Date of creation	2013-03-22 15:57:03
Last modified on	2013-03-22 15:57:03
Owner	Wkbj79 (1863)
Last modified by	Wkbj79 (1863)
Numerical id	15
Author	Wkbj79 (1863)
Entry type	Theorem
Classification	msc 16U99
Classification	msc 13A99
Classification	msc 13F10
Related topic	CyclicRing3
Related topic	PrincipalIdealRing
Related topic	MultiplicativeIdentityOfACyclicRingMustBeAGenerator
Related topic	CyclicRingsOfBehaviorOne

Theorem. *A cyclic ring is a principal ideal ring if and only if it has a multiplicative identity.*

Proof. Let R be a cyclic ring. If R has a multiplicative identity u, then u `http://planetmath.org/Generator`generates the additive group of R. Let I be an ideal of R. Since $\{0_R\}$ is principal, it may be assumed that I contains a nonzero element. Let n be the smallest natural number such that $nu \in I$. The inclusion $\langle nu \rangle \subseteq I$ is trivial. Let $t \in I$. Since $t \in R$, there exists $a \in \mathbb{Z}$ with $t = au$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $a = qn + r$. Thus, $t = au = (qn + r)u = (qn)u + ru = q(nu) + ru$. Since $ru = t - q(nu) \in I$, by choice of n, it must be the case that $r = 0$. Thus, $t = q(nu)$. Hence, $\langle nu \rangle = I$, and R is a principal ideal ring.

Conversely, if R is a principal ideal ring, then R is a principal ideal. Let k be the behavior of R and r be a `http://planetmath.org/Generator`generator of the additive group of R such that $r^2 = kr$. Since R is principal, there exists $s \in R$ such that $\langle s \rangle = R$. Let $a \in \mathbb{Z}$ such that $s = ar$. Since $r \in R = \langle s \rangle$, there exists $t \in R$ with $st = r$. Let $b \in \mathbb{Z}$ such that $t = br$. Then $r = st = (ar)(br) = (ab)r^2 = (ab)(kr) = (abk)r$. If R is infinite, then $abk = 1$, in which case $k = 1$ since k is nonnegative. If R is finite, then $abk \equiv 1 \operatorname{mod} |R|$, in which case $k = 1$ since k is a positive divisor of $|R|$. In either case, R has behavior one, and it follows that R has a multiplicative identity. $\square$