behavior exists uniquely (finite case)

Canonical name	BehaviorExistsUniquelyfiniteCase
Date of creation	2013-03-22 16:02:35
Last modified on	2013-03-22 16:02:35
Owner	Wkbj79 (1863)
Last modified by	Wkbj79 (1863)
Numerical id	13
Author	Wkbj79 (1863)
Entry type	Proof
Classification	msc 16U99
Classification	msc 13M05
Classification	msc 13A99

The following is a proof that behavior exists uniquely for any finite cyclic ring R.

Proof. Let n be the `http://planetmath.org/OrderRing`order of R and r be a `http://planetmath.org/Generator`generator of the additive group of R. Then there exists $a \in \mathbb{Z}$ with $r^2 = ar$. Let $k = \gcd(a, n)$ and $b \in \mathbb{Z}$ with $a = bk$. Since $\gcd(b, n) = 1$, there exists $c \in \mathbb{Z}$ with $bc \equiv 1 \bmod n$. Since $\gcd(c, n) = 1$, cr is a generator of the additive group of R. Since $(cr)^2 = c^2r^2 = c^2(ar) = c^2(bkr) = c(bc)(kr) = k(cr)$, it follows that k is a behavior of R. Thus, existence of behavior has been proven.

Let g and h be behaviors of R. Then there exist generators s and t of the additive group of R such that $s^2 = gs$ and $t^2 = ht$. Since t is a generator of the additive group of R, there exists $w \in \mathbb{Z}$ with $\gcd(w, n) = 1$ such that $t = ws$.

Note that $(hw)s = h(ws) = ht = t^2 = (ws)^2 = w^2s^2 = w^2(gs) = (gw^2)s$. Thus, $gw^2 \equiv hw \bmod n$. Recall that $\gcd(w, n) = 1$. Therefore, $gw \equiv h \bmod n$. Since g and h are both positive divisors of n and $\gcd(w, n) = 1$, it follows that $g = \gcd(g, n) = \gcd(gw, n) = \gcd(h, n) = h$. Thus, uniqueness of behavior has been proven. $\square$

Note that it has also been shown that, if R is a finite cyclic ring of order n, r is a generator of the additive group of R, and $a \in \mathbb{Z}$ with $r^2 = ar$, then the behavior of R is $\gcd(a, n)$.