Notebook problem #1

Jason Wojciechowski

15th April 2002

Theorem. *For every $n \in \mathbb{Z}$, there is exactly one ring with unity whose group under its first operation is $< \mathbb{Z}_n, + >$.*

Proof. Suppose B is a ring with unity such that $|B| = n$ and $< B, + > \cong < \mathbb{Z}_n, + >$. Let b_k be the multiplicative identity in B, and let it be isomorphic (from the addition group B to the addition group $\mathbb{Z}_n$) to k.

Then

$$b_k + b_k + b_k + b_k \cong k + k + k + k = 4k$$

under the isomorphism of the addition groups. However, since b_k is unity in B,

$$b_k + b_k + b_k + b_k = (b_k + b_k)(b_k + b_k)$$

so that, if the isomorphism established for the addition groups is to hold for the groups under multiplication, $(b_k + b_k)(b_k + b_k)$ must be isomorphic to $(k + k)(k + k) = 4k^2$ as well as to $4k$. This is only true if $k = 0$ or $k = 1$, but we know that unity can not be zero, so b_k must be isomorphic to $1 \in \mathbb{Z}$.

Thus any ring with unity whose first operation is $< \mathbb{Z}_n, + >$ is forced to have its multiplicative identity be isomorphic to $1 \in \mathbb{Z}_n$, so all such rings are isomorphic.

□