NAME:_________________________

Math 310.002 **Quiz 33** **Apr 18, 2012**

Prove: Any group G of order 2 is isomorphic to the cyclic group $(\mathbb{Z}_2, +)$. That is, there is a mapping $\phi : G \to \mathbb{Z}_2$ which turns the multiplication table of G into that of $\mathbb{Z}_2$.

Solution

- The order of a group, denoted $|G|$, is its number of elements. Thus, our G is any abstract group with 2 elements.

- The elements of G should be written as letters: symbols without any meaning as a symmetries, mappings, or matrices. The operation $*$ is unknown, but must fulfill Axioms (1)–(4), including the existence of an idenity e. Thus we may write $G = \{e, g\}$.

- A group always has only one operation, *not* addition and multiplication like a ring. We usually think of the group operation as a kind of multiplication, even when it is actually the addition of a ring, as for $(\mathbb{Z}_2, +)$. Thus, when I say "the multiplication tables of G and $\mathbb{Z}_2$," I mean the unknown $*$ operation for G, and the $+$ operation for $\mathbb{Z}_2$:

$$\begin{array}{c|cc} * & e & g \\ \hline e & e & g \\ g & g & ? \end{array} \qquad\qquad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

  Note that $(\mathbb{Z}_2, \cdot)$ is not a group at all: it is closed and associative, and 1 is the identity element, but 0 has no inverse with $0 \cdot a = 1$.

- We must have $g * g = e$, since g must have an inverse g^{-1}, and clearly $g^{-1} \neq e$, so the only other choice is $g^{-1} = g$, and $g * g = g * g^{-1} = e$.

- Now that we know the full table of G, we see that it is the same as the table of $\mathbb{Z}_2$ if we replace e by 0 and g by 1.

$$\begin{array}{c|cc} * & e & g \\ \hline e & e & g \\ g & g & e \end{array} \qquad\qquad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

- Put a second way, the mapping $\phi : G \to \mathbb{Z}_2$ with $\phi(e) = 0$ and $\phi(g) = 1$ is an isomorphism, because it is a bijection and takes every product $a * b = c$ in G to a corresponding valid equation $\phi(a) + \phi(b) = \phi(c)$ in $\mathbb{Z}_2$. That is:

$$\begin{array}{lcl} e * e = e & \text{becomes} & 0 + 0 = 0 \\ e * g = g & \text{becomes} & 0 + 1 = 1 \\ g * e = g & \text{becomes} & 1 + 0 = 1 \\ g * g = e & \text{becomes} & 1 + 1 = 1 \end{array}$$

  This is the formal definiton of a homomorphism: $\phi(a) + \phi(b) = \phi(a * b)$.