Group Maps Between Finite Cyclic Groups

Group maps \(Z_m \rightarrow Z_n\) are determined by the image of \(1 \in Z_m\): The image is an element whose order divides \((m, n)\), and all such elements are the image of such a group map.

**Theorem.**

(a) If \(f : Z_m \rightarrow Z_n\) is a group map, then \(\text{ord}\ f(1) \mid (m, n)\).

(b) If \(p \in Z_n\) satisfies \(\text{ord}\ p \mid (m, n)\), then there is a group map \(f : Z_m \rightarrow Z_n\) such that \(f(1) = p\).

**Proof.** (a) Suppose \(f : Z_m \rightarrow Z_n\) is a group map. Now \(m \cdot 1 = 0\) in \(Z_m\), so

\[m \cdot f(1) = f(m \cdot 1) = f(0) = 0.\]

This shows that \(\text{ord}\ f(1) \mid m\).

Since \(f(1) \in Z_n\), I have \(\text{ord}\ f(1) \mid n\).

Hence, \(\text{ord}\ f(1) \mid (m, n)\).

(b) Let \(p \in Z_n\), and suppose \(d = \text{ord}\ p \mid (m, n)\). Define \(g : Z \rightarrow Z_n\) by

\[g(x) = px.\]

Since \(d \mid m\), I have \(m = jd\) for some \(j \in Z\).

Now

\[
g(km) = \frac{pmk}{d} = \frac{pkjd}{d} \quad \text{(Since } m = jd)\]

\[= 0 \quad \text{(Since } \text{ord} p = d)\]

Since \(g\) sends \(m\mathbb{Z}\) to 0, the Universal Property of the Quotient produces a (unique) group map \(\tilde{g} : Z_m \rightarrow Z_n\) defined by

\[\tilde{g}(x) = px.\]

Then \(\tilde{g}(1) = p\), and \(\tilde{g}\) is the desired group map.  

**Corollary.** The number of group maps \(Z_m \rightarrow Z_n\) is \((m, n)\).

**Proof.** The number of elements of order \(d\) in a cyclic group is \(\phi(d)\) (where \(\phi\) denotes the Euler \(\phi\)-function).

The divisor sum of the Euler \(\phi\)-function is the identity:

\[
\sum_{d | k} \phi(d) = k.
\]

So the number of elements whose orders divide \((m, n)\) is \((m, n)\), and the theorem shows that each such element gives rise to a group map \(Z_m \rightarrow Z_n\).  

**Example.** (a) Enumerate the group maps \(Z_{18} \rightarrow Z_{30}\).

(b) Show by direct computation that \(f : Z_{18} \rightarrow Z_{30}\) given by \(f(x) = 14x\) is not a group map.

(a) Since \((18, 30) = 6\), there are 6 such maps by the Corollary. They are determined by sending \(1 \in Z_{18}\) to an element whose order divides 6.

<table>
<thead>
<tr>
<th>order</th>
<th>elements in (Z_{30}) of that order</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>10, 20</td>
</tr>
<tr>
<td>6</td>
<td>5, 25</td>
</tr>
</tbody>
</table>

1
Thus, the possible group maps $f : \mathbb{Z}_{18} \to \mathbb{Z}_{30}$ have

$$f(1) = 0, \quad f(1) = 15, \quad f(1) = 10, \quad f(1) = 20, \quad f(1) = 5, \quad f(1) = 25.$$  

For example, the group map

$$f(x) = 20x$$

has $f(1) = 20$.

It is easy to determine the kernel and the image. The image is the unique subgroup of $\mathbb{Z}_{30}$ of order 3, so

$$\text{im } f = \{0, 10, 20\}.$$  

By the First Isomorphism Theorem, the kernel must have order $\frac{18}{3} = 6$. The unique subgroup of $\mathbb{Z}_{18}$ of order 6 is

$$\ker f = \{0, 3, 6, 9, 12, 15\}.$$  

(b) Consider the function $f : \mathbb{Z}_{18} \to \mathbb{Z}_{30}$ given by $f(x) = 14x$. Then

$$f(3 + 15) = f(0) = 0, \quad \text{but} \quad f(3) + f(15) = 12 + 0 = 12.$$  

Therefore, $f(3 + 15) \neq f(3) + f(15)$, so $f$ is not a group map. ☐