Group Maps Between Finite Cyclic Groups

Group maps $\mathbb{Z}_m \to \mathbb{Z}_n$ are determined by the image of $1 \in \mathbb{Z}_m$: 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 $f : \mathbb{Z}_m \to \mathbb{Z}_n$ is a group map, then $\operatorname{ord} f(1) \mid (m, n)$.

(b) If $p \in \mathbb{Z}_n$ satisfies $\operatorname{ord} p \mid (m, n)$, then there is a group map $f : \mathbb{Z}_m \to \mathbb{Z}_n$ such that $f(1) = p$.

Proof. (a) Suppose $f : \mathbb{Z}_m \to \mathbb{Z}_n$ is a group map. Now $m \cdot 1 = 0$ in $\mathbb{Z}_m$, so

$$m \cdot f(1) = f(m \cdot 1) = f(0) = 0.$$

This shows that $\operatorname{ord} f(1) \mid m$.
Since $f(1) \in \mathbb{Z}_n$, I have $\operatorname{ord} f(1) \mid n$.
Hence, $\operatorname{ord} f(1) \mid (m, n)$.

(b) Let $p \in \mathbb{Z}_n$, and suppose $d = \operatorname{ord} p \mid (m, n)$. Define $g : \mathbb{Z} \to \mathbb{Z}_n$ by

$$g(x) = px.$$

Since $d \mid m$, I have $m = jd$ for some $j \in \mathbb{Z}$.
Now

$$\begin{aligned} g(km) &= pkm \\ &= pk(jd) \quad \text{(Since } m = jd\text{)} \\ &= 0 \quad \text{(Since } \operatorname{ord} p = d\text{)} \end{aligned}$$

Since g sends $m\mathbb{Z}$ to 0, the Universal Property of the Quotient produces a (unique) group map $\tilde{g} : \mathbb{Z}_m \to \mathbb{Z}_n$ 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 $\mathbb{Z}_m \to \mathbb{Z}_n$ is (m, n).

Proof. The number of elements of order d in a cyclic group is $\phi(d)$ (where ϕ denotes the Euler ϕ-function). The divisor sum of the Euler ϕ-function is the identity:

$$\sum_{d \mid k} \phi(d) = k.$$

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 $\mathbb{Z}_m \to \mathbb{Z}_n$. □

Example. (a) Enumerate the group maps $\mathbb{Z}_{18} \to \mathbb{Z}_{30}$.

(b) Show by direct computation that $f : \mathbb{Z}_{18} \to \mathbb{Z}_{30}$ 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 $1 \in \mathbb{Z}_{18}$ to an element whose order divides 6.

order	elements in $\mathbb{Z}_{30}$ of that order
1	0
2	15
3	10, 20
6	5, 25

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

$$f(x) = 20x \quad \text{has} \quad f(1) = 20.$$

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

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

By the First Isomorphism Theorem, the kernel must have order $\dfrac{18}{3} = 6$. 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. $\square$
