Homomorphisms and Generating Sets

Holden Swindell

Suppose that F is a field and that V and W are vector spaces over F. Given a basis $\mathcal{B}$ for V, we can construct a linear map $T : V \to W$ by specifying its value on each element of the basis $\mathcal{B}$. This specification uniquely determines T. Formally, we have the following theorem:

Theorem 1. *Let F be a field and V and W be vector spaces over F. Suppose that $\mathcal{B} \subseteq V$ is a basis for V and that $t : \mathcal{B} \to W$ is a function. There then exists a unique linear map $T : V \to W$ such that $T(v) = t(v)$ for all $v \in \mathcal{B}$.*

Now suppose that G is a group and that S is a generating set for G, i.e, $\langle S \rangle = G$. One might expect that a result analogous to Theorem 1 also holds, in that we can construct a homomorphism out of G by specifying its value on each element of S. Formally, we might expect that the following theorem holds:

(Potential) Theorem 2. *Let G and H be groups and $S \subseteq G$ be a generating set for G. Suppose that $\phi : S \to H$ is a function. There then exists a unique homomorphism $\Phi : G \to H$ such that $\Phi(s) = \phi(s)$ for all $s \in S$.*

Unfortunately, Theorem 2 is false. Set $G = H = \mathbb{Z}$, so that $S = \{1, 2\}$ is a generating set for G. Define $\phi : S \to H$ by $\phi(1) = \phi(2) = 2$. If there was a homomorphism $\Phi : G \to H$ that extends ϕ, then

$$\begin{aligned} 0 &= \Phi(0) && (1)\\ &= \Phi(2 - 1 - 1) && (2)\\ &= \Phi(2) - \Phi(1) - \Phi(1) && (3)\\ &= \phi(2) - \phi(1) - \phi(1) && (4)\\ &= 2 - 2 - 2 && (5)\\ &= -2, && (6) \end{aligned}$$

a contradiction.

How should we fix Theorem 2? The solution is suggested by the preceding counterexample. The issue was that ϕ didn't respect the relation $2 - 1 - 1 = 0$, in that $\phi(2) - \phi(1) - \phi(1) \neq 0$. Furthermore, any function ϕ would have to respect this relation in order to extend to a homomorphism Φ. We then might guess that a function ϕ extends to a homomorphism Φ if and only if it respects all the relations between elements of S, i.e, if elements of S combine to form

the identity element e_G, then their images under ϕ combine to form the identity element e_H. Indeed, we have the following (correct) version of Theorem 2:

Theorem 3. *Let G and H be groups and $S \subseteq G$ be a generating set for G. Suppose that $\phi : S \to H$ is a function. The following are equivalent:*

1. *There exists a homomorphism $\Phi : G \to H$ such that $\Phi(s) = \phi(s)$ for all $s \in S$;*
2. *For every positive integer n, $s_1, \ldots, s_n \in S$, and $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$, if $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} = e_G$, then $\phi(s_1)^{\varepsilon_1} \cdots \phi(s_n)^{\varepsilon_n} = e_H$.*

Furthermore, if there does exist a homomorphism $G \to H$ extending ϕ, it is unique.

Proof. (1) $\Rightarrow$ (2): Let n be a positive integer, $s_1, \ldots, s_n \in S$, and $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$. Assume that $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} = e_G$. Since Φ extends ϕ and is a homomorphism, we have that

$$\phi(s_1)^{\varepsilon_1} \cdots \phi(s_n)^{\varepsilon_n} = \Phi(s_1)^{\varepsilon_1} \cdots \Phi(s_n)^{\varepsilon_n} = \Phi(s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}) = \Phi(e_G) = e_H. \quad (7)$$

(1) $\Leftarrow$ (2): Define a function $\Phi : G \to H$ as follows. First, define $\Phi(e_G) = e_H$. Next, if $g \in G$ and $g \neq e_G$, then since S generates G there exists a positive integer n, $s_1, \ldots, s_n \in S$, and $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$ such that $g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$. Define

$$\Phi(g) = \phi(s_1)^{\varepsilon_1} \cdots \phi(s_n)^{\varepsilon_n}. \quad (8)$$

We now verify that Φ is well-defined. Suppose that $g \in G$ and that $g \neq e_G$. Suppose also that n and m are positive integers, $a_1, \ldots, a_n, b_1, \ldots, b_m \in S$, and $\varepsilon_1, \ldots, \varepsilon_n, \delta_1, \ldots, \delta_m \in \{1, -1\}$ are such that

$$g = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} = b_1^{\delta_1} \cdots b_m^{\delta_m}. \quad (9)$$

Then

$$a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} b_m^{-\delta_m} \cdots b_1^{-\delta_1} = e_G, \quad (10)$$

and so by assumption

$$\phi(a_1)^{\varepsilon_1} \cdots \phi(a_n)^{\varepsilon_n} \phi(b_m)^{-\delta_m} \cdots \phi(b_1)^{-\delta_1} = e_H. \quad (11)$$

Therefore

$$\phi(a_1)^{\varepsilon_1} \cdots \phi(a_n)^{\varepsilon_n} = \phi(b_1)^{\delta_1} \cdots \phi(b_m)^{\delta_m} \quad (12)$$

and Φ is well-defined.

Next, we verify that Φ is a homomorphism. Let $a, b \in G$. If $a = e_G$, then

$$\Phi(ab) = \Phi(e_G b) = \Phi(b) = e_H \Phi(b) = \Phi(e_G)\Phi(b) = \Phi(a)\Phi(b), \quad (13)$$

and if $b = e_G$,

$$\Phi(ab) = \Phi(ae_G) = \Phi(a) = \Phi(a)e_H = \Phi(a)\Phi(e_G) = \Phi(a)\Phi(b). \quad (14)$$

We can then assume that $a \neq e_G$ and $b \neq e_G$. There then exist positive integers n and m, $a_1, \ldots, a_n, b_1, \ldots, b_m \in S$, and $\varepsilon_1, \ldots, \varepsilon_n, \delta_1, \ldots, \delta_m \in \{1, -1\}$ such that $a = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ and $b = b_1^{\delta_1} \cdots b_m^{\delta_m}$. By definition,

$$\begin{aligned}
\Phi(ab) &= \Phi(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} b_1^{\delta_1} \cdots b_m^{\delta_m}) && (15)\\
&= \phi(a_1)^{\varepsilon_1} \cdots \phi(a_n)^{\varepsilon_n} \phi(b_1)^{\delta_1} \cdots \phi(b_m)^{\delta_m} && (16)\\
&= \Phi(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}) \Phi(b_1^{\delta_1} \cdots b_m^{\delta_m}) && (17)\\
&= \Phi(a)\Phi(b). && (18)
\end{aligned}$$

Therefore $\Phi(ab) = \Phi(a)\Phi(b)$ in all cases, so Φ is a homomorphism.

We also need to verify that Φ extends ϕ. Let $s \in S$. If $s = e_G$, then $s^1 = e_G$, so by assumption $\phi(s)^1 = e_H$. By the definition of Φ,

$$\Phi(s) = \Phi(e_G) = e_H = \phi(s)^1 = \phi(s). \tag{19}$$

If $s \neq e_G$, then since $s = s^1$, by the definition of Φ,

$$\Phi(s) = \phi(s)^1 = \phi(s). \tag{20}$$

Therefore $\Phi(s) = \phi(s)$ in both cases.

This proves the equivalence (1) $\iff$ (2).

Finally, we prove uniqueness. Suppose that $\Phi, \Psi : G \to H$ are homomorphisms such that $\Phi(s) = \phi(s) = \Psi(s)$ for all $s \in S$. Then, if

$$K = \{g \in G : \Phi(g) = \Psi(g)\}, \tag{21}$$

we have that $S \subseteq K$. We claim that $K \leq G$. First, since Φ and Ψ are homomorphisms, $\Phi(e_G) = e_H = \Psi(e_G)$ and $e_G \in K$. Next, if $a, b \in K$, then

$$\Phi(ab) = \Phi(a)\Phi(b) = \Psi(a)\Psi(b) = \Psi(ab) \tag{22}$$

and $ab \in K$. Finally, if $a \in K$, then

$$\Phi(a^{-1}) = \Phi(a)^{-1} = \Psi(a)^{-1} = \Psi(a^{-1}) \tag{23}$$

and $a^{-1} \in K$. Therefore $K \leq G$, and since $S \subseteq K$, $G = \langle S \rangle \subseteq K$. Thus $K = G$ and $\Phi = \Psi$. □

Verifying the second condition of Theorem 3 can often be made easier by choosing more "optimal" generating sets. This is particularly the case for cyclic groups. Indeed, the following two results can be proven using Theorem 3 and are in fact special cases of it:

Theorem 4. *Let G be a group and $g_0 \in G$. There then exists a unique homomorphism $\Phi : \mathbb{Z} \to G$ such that $\Phi(1) = g_0$.*

Theorem 5. *Let G be a group and $g_0 \in G$. Suppose that n is an integer with $n \geq 2$. The following are equivalent:*

1. *There exists a homomorphism $\Phi : \mathbb{Z}/n\mathbb{Z} \to G$ such that $\Phi(\bar{1}) = g_0$;*
2. *$g_0^n = e_G$.*

What explains the discrepancy between Theorem 1 and Theorem 3? The culprit is that a basis for a vector space has to satisfy two conditions: spanning and linear independence. For groups, a generating set satisfies an analogous spanning condition, but has no analogous linear independence requirement. We would get a result for vector spaces analogous to Theorem 3 if we only assumed that we had a spanning set.

Similar results can be proven for generating sets of modules and rings. This suggests that there might be a generalization of all these results to the setting of category theory, likely using the concept of a generator of a category.