

# UNIVERSAL MAPPING PROPERTIES

KEITH CONRAD

The construction of a new algebraic object from old ones is often defined by formulas for the elements of the new object and operations in it. Two examples are quotient groups  $G/N$  and product groups  $G_1 \times G_2$ :  $G/N$  consists of cosets  $gN$  multiplied by the rule  $gN \cdot g'N = gg'N$  and  $G_1 \times G_2$  consists of ordered pairs  $(g_1, g_2)$  with  $g_i \in G_i$  and operations defined componentwise.

There is another way to describe such constructions: say how the new object is related (by mappings) to all other objects of a similar type. This lets us characterize a new object up to a *unique* isomorphism. Studying mathematical objects by their interactions with similar objects, rather than by an explicit construction of the object, is analogous to studying elementary particles by smashing them together (except math is much less expensive). Our examples will be from group theory, ring theory, and module theory.

- Group theory: cyclic groups, quotient groups, abelianizations, direct products
- Ring theory: quotient ring, direct product, fraction field
- Module theory: cyclic modules, quotient modules, direct products, direct sums, and free modules.

In an appendix we discuss the universal mapping property for the product topology, quotient topology, and completion of a metric space.

## 1. CYCLIC GROUPS

Fix  $n \geq 1$ . All cyclic groups of order  $n$  (e.g.  $\mathbf{Z}/n\mathbf{Z}$  and  $\mu_n$ ) are isomorphic, but not uniquely: the isomorphism depends on a *choice* of generator in each group. Changing the generator of either group changes the isomorphism between the groups.

**Example 1.1.** The groups  $\mu_{10}$  and  $(\mathbf{Z}/11\mathbf{Z})^\times$  are both cyclic of order 10. A generator of  $\mu_{10}$  is  $\zeta = e^{2\pi i/10}$ . The generators of  $(\mathbf{Z}/11\mathbf{Z})^\times$  are 2, 6, 7, and 8, and each choice leads to a different isomorphism  $\mu_{10} \rightarrow (\mathbf{Z}/11\mathbf{Z})^\times$ :

$$f_1(\zeta^a) = 2^a \pmod{11}, \quad f_2(\zeta^a) = 6^a \pmod{11}, \quad f_3(\zeta^a) = 7^a \pmod{11}, \quad f_4(\zeta^a) = 8^a \pmod{11}.$$

**Theorem 1.2.** *Let  $C$  be a cyclic group of order  $n$  with generator  $c$ .*

- (1) *For each group  $G$  and  $\gamma \in G$  such that  $\gamma^n = 1$ , there is a unique homomorphism  $f: C \rightarrow G$  such that  $f(c) = \gamma$ .*
- (2) *If  $G$  is cyclic of order  $n$  and  $\gamma$  in  $G$  has order  $n$  then  $f$  in (1) is an isomorphism.*

Saying  $\gamma^n = 1$  means  $\gamma$  has order dividing  $n$ , not order equal to  $n$ . Perhaps  $\gamma = 1$ .

*Proof.* Since each element of  $C$  is a power of  $c$ , a homomorphism  $C \rightarrow G$  is completely determined by its value on  $c$ . If  $f: C \rightarrow G$  is a homomorphism such that  $f(c) = \gamma$ , then  $f(c^j) = \gamma^j$  for all  $j$ . This formula is a group homomorphism:

- the definition of  $f(c^j)$  makes sense, since  $c^j = c^{j'} \Rightarrow j \equiv j' \pmod{n}$  ( $c$  has order  $n$ ), which implies  $\gamma^j = \gamma^{j'}$  (since  $\gamma^n = 1$ ),

- $f$  is a homomorphism since all elements of  $C$  are powers of  $c$  and  $f(c^j c^k) = f(c^{j+k}) = \gamma^{j+k} = \gamma^j \gamma^k = f(c^j) f(c^k)$ .

If  $G$  is cyclic of order  $n$  and  $\gamma$  has order  $n$  then  $f(C) = \langle f(c) \rangle = \langle \gamma \rangle = G$ , so  $f$  is surjective. A surjective homomorphism of two finite groups of equal order is injective, so  $f$  is an isomorphism.  $\square$

This theorem is telling us that by including the choice of generator of  $C$  as part of the data we keep track of, we rigidified the situation: there is exactly one homomorphism. Let's consider all pairs  $(G, \gamma)$  where  $G$  is a group and  $\gamma$  is an element of  $G$  such that  $\gamma^n = 1$ .

**Definition 1.3.** A pair  $(G, \gamma)$  where  $\gamma^n = 1$  is called an  $n$ -marked group. If  $G$  is cyclic of order  $n$  and  $\gamma$  generates  $G$  then  $(G, \gamma)$  is called a *cyclic  $n$ -marked group*.

**Example 1.4.** Some  $n$ -marked groups are  $(\mathbf{Z}/n\mathbf{Z}, a)$  for each  $a \in \mathbf{Z}/n\mathbf{Z}$ ,  $(\mathbf{C}^\times, \zeta)$  where  $\zeta$  is an  $n$ th root of unity in  $\mathbf{C}$ , and  $(G, e)$ , for arbitrary  $G$ . When  $n = 4$ ,  $(S_5, (12))$  is an example. If  $(G, \gamma)$  is an  $n$ -marked group, so is  $(G, \gamma^a)$  for each integer  $a$ , since  $(\gamma^a)^n = (\gamma^n)^a = 1$ .

The  $n$ -marked group  $(\mathbf{Z}/n\mathbf{Z}, a)$  is a cyclic  $n$ -marked group only when  $(a, n) = 1$  because that is when  $a$  generates  $\mathbf{Z}/n\mathbf{Z}$ .

**Definition 1.5.** A *morphism* of  $n$ -marked groups  $f: (G_1, \gamma_1) \rightarrow (G_2, \gamma_2)$  is a group homomorphism  $f: G_1 \rightarrow G_2$  such that  $f(\gamma_1) = \gamma_2$ .

**Example 1.6.** For each  $n$ -marked group  $(G, \gamma)$ , the identity mapping  $\text{id}: G \rightarrow G$  gives us a morphism  $(G, \gamma) \rightarrow (G, \gamma)$ .

**Example 1.7.** For the 4-marked groups  $(\mu_4, i)$  and  $(\mathbf{R}^\times, -1)$ , the mapping  $f: (\mu_4, i) \rightarrow (\mathbf{R}^\times, -1)$  where  $f(i^k) = (-1)^k$  is a morphism. There is no morphism in the other direction  $(\mathbf{R}^\times, -1) \rightarrow (\mu_4, i)$  since it would be a homomorphism  $\mathbf{R}^\times \rightarrow \mu_4$  mapping  $-1$  to  $i$  and a group homomorphism can't send an element of order 2 to an element of order 4. (There are homomorphisms  $\mathbf{R}^\times \rightarrow \mu_4$ , such as  $x \mapsto \text{sign}(x)$ , or the trivial homomorphism  $x \mapsto 1$ , but there is none sending  $-1$  to  $i$ .)

**Example 1.8.** A composition of morphisms is a morphism: if  $f_1: (G_1, \gamma_1) \rightarrow (G_2, \gamma_2)$  and  $f_2: (G_2, \gamma_2) \rightarrow (G_3, \gamma_3)$  are morphisms then  $f_2 \circ f_1: G_1 \rightarrow G_3$  is a group homomorphism such that  $(f_2 \circ f_1)(\gamma_1) = f_2(f_1(\gamma_1)) = f_2(\gamma_2) = \gamma_3$ , so we have a morphism  $f_2 \circ f_1: (G_1, \gamma_1) \rightarrow (G_3, \gamma_3)$ .

Using this new terminology of morphisms of  $n$ -marked groups, we can express the first part of Theorem 1.2 as follows. If  $(C, c)$  is a cyclic  $n$ -marked group then

*for every  $n$ -marked group  $(G, \gamma)$ , there is a unique morphism  $(C, c) \rightarrow (G, \gamma)$ .*

That we can map a cyclic  $n$ -marked group  $(C, c)$  to each  $n$ -marked group in exactly one way (by a morphism, not a random function) is called the *universal mapping property* of cyclic  $n$ -marked groups (cyclic groups of order  $n$  with a choice of generator). The term "universal" refers to  $(C, c)$  being related to every  $n$ -marked group.

**Example 1.9.** If  $(C, c)$  is a cyclic  $n$ -marked group then the unique morphism  $(C, c) \rightarrow (C, c)$  is the identity mapping on  $C$ . In concrete terms, this is saying that a homomorphism  $C \rightarrow C$  that fixes  $c$  has to fix all powers of  $c$  and thus fixes all of  $C$  since  $C = \langle c \rangle$ .

Now we reach a key point: two  $n$ -marked groups satisfying the universal mapping property above are isomorphic in a unique way respecting their chosen elements of order  $n$ .

**Theorem 1.10.** *If  $(A, a)$  and  $(B, b)$  are  $n$ -marked groups that satisfy the universal mapping property of cyclic  $n$ -marked groups then the unique morphism  $(A, a) \rightarrow (B, b)$  is a group isomorphism  $A \rightarrow B$  sending  $a$  to  $b$ .*

*Proof.* Pay close attention to this argument. It makes no use of the group structure of  $A$  or  $B$ . The uniqueness aspect of the universal mapping property is all we need to rely on.

By the universal mapping property of cyclic  $n$ -marked groups, there are unique morphisms  $f: (A, a) \rightarrow (B, b)$  and  $f': (B, b) \rightarrow (A, a)$ . The compositions  $f' \circ f: (A, a) \rightarrow (A, a)$  and  $f \circ f': (B, b) \rightarrow (B, b)$  are morphisms (Example 1.8). The identity morphisms  $(A, a) \rightarrow (A, a)$  and  $(B, b) \rightarrow (B, b)$  also exist (Example 1.9), so by uniqueness  $f' \circ f = \text{id}_A$  and  $f \circ f' = \text{id}_B$ .  $\square$

Since we know cyclic  $n$ -marked groups  $(C, c)$  really exist and they satisfy the universal mapping property of cyclic  $n$ -marked groups, the isomorphism in Theorem 1.10 tells us that every  $n$ -marked group  $(A, a)$  satisfying the universal mapping property of cyclic  $n$ -marked group has  $A$  cyclic of order  $n$  and  $\langle a \rangle = A$ . Bare cyclic groups of order  $n$  are not characterized by a universal mapping property. Cyclic groups of order  $n$  *together with a choice of generator* (i.e., cyclic  $n$ -marked groups of order  $n$ ) are being characterized.

**Definition 1.11.** An *isomorphism* of  $n$ -marked groups  $f: (G_1, \gamma_1) \rightarrow (G_2, \gamma_2)$  is a morphism  $(G_1, \gamma_1) \rightarrow (G_2, \gamma_2)$  that is bijective as a function from  $G_1$  to  $G_2$ .

This means  $f: G_1 \rightarrow G_2$  is a group isomorphism and  $f(\gamma_1) = \gamma_2$ . The inverse isomorphism  $f^{-1}$  is an isomorphism  $(G_2, \gamma_2) \rightarrow (G_1, \gamma_1)$  since it is bijective and  $f^{-1}(\gamma_2) = \gamma_1$ .

Using this terminology, two cyclic  $n$ -marked groups have a unique isomorphism between them. This is often expressed by saying a cyclic  $n$ -marked group is “unique up to unique isomorphism” and it is a fancy way of expressing the second part of Theorem 1.2.

## 2. QUOTIENT GROUPS

We turn now to quotient groups. Fix a group  $G$  and normal subgroup  $N \triangleleft G$ . For the quotient group  $G/N$ , the reduction homomorphism  $\pi_N: G \rightarrow G/N$  that sends  $g$  to  $gN$  has kernel  $N$ . An important property of  $G/N$  with  $\pi_N$  is: when  $G \xrightarrow{f} \tilde{G}$  is a homomorphism from  $G$  to an arbitrary group  $\tilde{G}$  such that  $f$  is trivial on  $N$  ( $N \subset \ker f$ ), there is a *unique* homomorphism  $\bar{f}: G/N \rightarrow \tilde{G}$  making the following diagram commute (“ $f$  factors through the quotient”).

$$\begin{array}{ccc} G & \xrightarrow{f} & \tilde{G} \\ & \searrow \pi_N & \nearrow \bar{f} \\ & G/N & \end{array}$$

The reason  $\bar{f}$  is unique is that commutativity says  $\bar{f}(gN) = f(g)$  for all  $g \in G$  and every element of  $G/N$  is some  $gN$ , so  $\bar{f}$  is completely determined.

It is useful to rotate the above diagram to put  $\pi_N$  and  $f$  on a more equal footing.

(2.1)

$$\begin{array}{ccc} & G & \\ \pi_N \swarrow & & \searrow f \\ G/N & \xrightarrow{\bar{f}} & \tilde{G} \end{array}$$

Think of  $\bar{f}$  in (2.1) as sending the pair  $(G/N, \pi_N)$  to the pair  $(\tilde{G}, f)$ .

**Definition 2.1.** An  $N$ -trivial group is a pair  $(\tilde{G}, f)$  where  $\tilde{G}$  is a group and  $f: G \rightarrow \tilde{G}$  is a homomorphism to  $\tilde{G}$  that is trivial on  $N$ .

An example of an  $N$ -trivial group is  $(G/N, \pi_N)$ . Another is  $(\tilde{G}, f)$  for arbitrary  $\tilde{G}$  and  $f: G \rightarrow \tilde{G}$  is the trivial homomorphism that sends all of  $G$  to the identity in  $\tilde{G}$ .

**Definition 2.2.** For two  $N$ -trivial groups  $(G_1, f_1)$  and  $(G_2, f_2)$ , a *morphism* from the first to the second is a homomorphism  $G_1 \xrightarrow{h} G_2$  such that the following diagram commutes.

$$\begin{array}{ccc} & G & \\ f_1 \swarrow & & \searrow f_2 \\ G_1 & \xrightarrow{h} & G_2 \end{array}$$

We call this morphism  $h$  an *isomorphism* if it is an isomorphism from  $G_1$  to  $G_2$ .

**Example 2.3.** For an  $N$ -trivial group  $(\tilde{G}, f)$ , the identity mapping on  $\tilde{G}$  defines a morphism

$$\begin{array}{ccc} & G & \\ f \swarrow & & \searrow f \\ \tilde{G} & \xrightarrow{\text{id}} & \tilde{G} \end{array}$$

and we call this the identity morphism of  $(\tilde{G}, f)$ . This is an analogue of Example 1.6.

**Example 2.4.** The composition of two morphisms is a morphism: if  $h_1: (G_1, f_1) \rightarrow (G_2, f_2)$  and  $h_2: (G_2, f_2) \rightarrow (G_3, f_3)$  are morphisms of  $N$ -trivial groups then in the left diagram

$$\begin{array}{ccccc} & G & & G & \\ & \swarrow f_1 & \downarrow f_2 & \swarrow f_1 & \searrow f_3 \\ G_1 & \xrightarrow{h_1} & G_2 & \xrightarrow{h_2} & G_3 \\ & & & & h_2 \circ h_1 \end{array}$$

the left triangle and right triangle commute, so the big triangle commutes:

$$(h_2 \circ h_1) \circ f_1 = h_2 \circ (h_1 \circ f_1) = h_2 \circ f_2 = f_3.$$

Thus the diagram on the right, where the middle arrow has been removed, is commutative, so  $h_2 \circ h_1: (G_1, f_1) \rightarrow (G_3, f_3)$  is a morphism. This is an analogue of Example 1.8.

The uniqueness of  $\bar{f}$  fitting in (2.1) is called the *universal mapping property* of  $G/N$  (really, of  $G/N$  together with  $\pi_N: G \rightarrow G/N$ ). This refers to the following property.

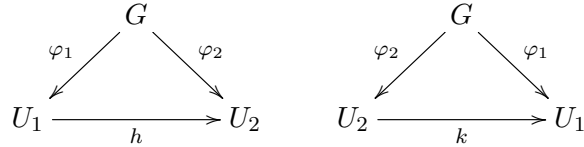
**Definition 2.5.** An  $N$ -trivial group  $(U, \varphi)$  is called *universal* if for each  $N$ -trivial group  $(\tilde{G}, f)$ , there is a unique morphism  $(U, \varphi) \rightarrow (\tilde{G}, f)$ : there is a unique homomorphism  $U \rightarrow \tilde{G}$  making the following diagram commute.

$$\begin{array}{ccc} & G & \\ \varphi \swarrow & & \searrow f \\ U & \cdots \cdots \cdots & \tilde{G} \end{array}$$

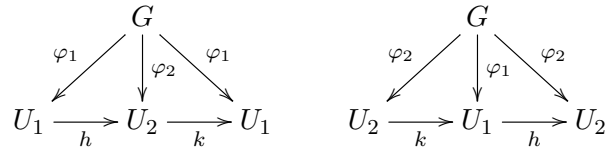
One universal  $N$ -trivial group is  $(G/N, \pi_N)$ . Let's show all others are isomorphic to it.

**Theorem 2.6.** *If  $(U_1, \varphi_1)$  and  $(U_2, \varphi_2)$  are universal  $N$ -trivial groups then there is a unique morphism  $(U_1, \varphi_1) \rightarrow (U_2, \varphi_2)$  and it is an isomorphism.*

*Proof.* Since  $(U_1, \varphi_1)$  and  $(U_2, \varphi_2)$  are universal  $N$ -trivial groups, there is a unique morphism from each to the other: we have commutative diagrams



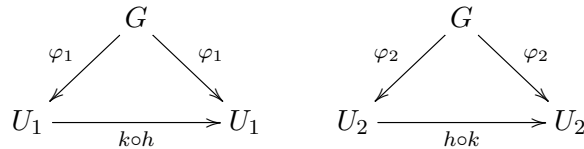
for unique group homomorphisms  $h$  and  $k$ . We'll show  $h$  and  $k$  are inverses, so in fact they are group isomorphisms. Put the diagrams above together in two ways to get new diagrams.



In these diagrams the smaller triangles commute, so the big ones commute. For example,

$$(k \circ h) \circ \varphi_1 = k \circ (h \circ \varphi_1) = k \circ \varphi_2 = \varphi_1.$$

Now remove the middle parts of the diagrams to get the following commutative diagrams.



Since  $(U_1, \varphi_1)$  is a universal  $N$ -trivial group, only one homomorphism can appear where  $k \circ h$  does in the first commutative diagram. Since  $\text{id}_{U_1}$  fits,  $k \circ h = \text{id}_{U_1}$ . Similarly,  $h \circ k = \text{id}_{U_2}$  by the second commutative diagram and  $(U_2, \varphi_2)$  being a universal  $N$ -trivial group. Thus  $U_1 \cong U_2$  by inverse group isomorphisms  $h$  and  $k$ .

$$U_1 \begin{array}{c} \xleftarrow{k} \\ \xrightarrow{h} \end{array} U_2 \qquad \square$$

Here is a “practical” use of universal  $N$ -trivial groups being isomorphic to each other.

**Theorem 2.7.** *For a group  $G$ , let  $N$  and  $N'$  be normal subgroups such that  $N' \subset N \subset G$ . Then  $(G/N')/(N/N') \cong G/N$  as groups.*

*Proof.* The composition  $G \xrightarrow{\pi_{N'}} G/N' \xrightarrow{\bar{\pi}} (G/N')/(N/N')$ , where  $\pi_{N'}$  and  $\bar{\pi}$  are reduction maps, is a homomorphism trivial on  $N$ , so  $((G/N')/(N/N'), \bar{\pi} \circ \pi_{N'})$  is an  $N$ -trivial group. We'll show this  $N$ -trivial group is *universal*. Then, since  $(G/N, \pi_N)$  is also a universal  $N$ -trivial group,  $(G/N')/(N/N') \cong G/N$  by Theorem 2.6.

Let  $G \xrightarrow{f} \tilde{G}$  be a homomorphism that is trivial on  $N$ . Since  $N' \subset N$ ,  $f$  is trivial on  $N'$ , so there is a unique homomorphism  $f': G/N' \rightarrow \tilde{G}$  making the following diagram commute.

$$\begin{array}{ccc} & G & \\ \pi_{N'} \swarrow & & \searrow f \\ G/N' & \xrightarrow{f'} & \tilde{G} \end{array}$$

The mapping  $f'$  is trivial on  $N/N'$  since  $f'(nN') = f'(\pi_{N'}(n)) = f(n)$ , which is trivial. So a unique homomorphism  $f'': (G/N')/(N/N') \rightarrow \tilde{G}$  makes the following diagram commute, where  $\bar{\pi}$  is a reduction map.

$$\begin{array}{ccc} & G/N' & \\ \bar{\pi} \swarrow & & \searrow f' \\ (G/N')/(N/N') & \xrightarrow{f''} & \tilde{G} \end{array}$$

Sticking these diagrams together creates the following larger commutative diagram on the left, which we simplify on the right by removing anything directly involving  $G/N'$ .

$$\begin{array}{ccc} & G & \\ & \swarrow \pi_{N'} & \downarrow f \\ & G/N' & \\ \bar{\pi} \swarrow & & \searrow f' \\ (G/N')/(N/N') & \xrightarrow{f''} & \tilde{G} \end{array} \qquad \begin{array}{ccc} & G & \\ & \swarrow \bar{\pi} \circ \pi_{N'} & \downarrow f \\ & (G/N')/(N/N') & \xrightarrow{f''} \tilde{G} \end{array}$$

Therefore to each  $N$ -trivial group  $(\tilde{G}, f)$  there is a homomorphism  $f'': (G/N')/(N/N') \rightarrow \tilde{G}$  such that  $f'' \circ (\bar{\pi} \circ \pi_{N'}) = f$ . This means, for each  $g \in G$ , that

$$f(g) = f''((\bar{\pi} \circ \pi_{N'})(g)) = f''(\bar{\pi}(gN')) = f''(\bar{g}N/N'),$$

where  $\bar{g} = gN'$ . Each element of  $(G/N')/(N/N')$  is  $\bar{g}N/N'$  for some  $g$ , so  $f''$  is determined by fitting in the commutative diagram on the right. Thus  $f''$  is the only homomorphism such that  $f'' \circ (\bar{\pi} \circ \pi_{N'}) = f$ , making the  $N$ -trivial group  $((G/N')/(N/N'), \bar{\pi} \circ \pi_{N'})$  universal.  $\square$

**Remark 2.8.** Since  $((G/N')/(N/N'), \bar{\pi} \circ \pi_{N'})$  and  $(G/N, \pi_N)$  are both universal  $N$ -trivial groups, there is a unique isomorphism  $h: (G/N')/(N/N') \rightarrow G/N$  making the diagram

$$\begin{array}{ccc} & G & \\ \bar{\pi} \circ \pi_{N'} \swarrow & & \searrow \pi_N \\ (G/N')/(N/N') & \xrightarrow{h} & G/N \end{array}$$

commute, by Theorem 2.6. Commutativity means, for each  $g \in G$ , that

$$h((\bar{\pi} \circ \pi_{N'})(g)) = \pi_N(g) \implies h(\bar{\pi}(gN')) = gN \implies \boxed{h(\bar{g}N/N') = gN},$$

where  $\bar{g} = gN'$ . The formula in the box is the isomorphism  $(G/N')/(N/N') \rightarrow G/N$  seen in an algebra course where these groups are proved isomorphic as part of the isomorphism theorems for groups without mentioning universal mapping properties.

A way to think about the isomorphism  $h: (U_1, \varphi_1) \rightarrow (U_2, \varphi_2)$  between two universal  $N$ -trivial groups is that the commutativity of

$$\begin{array}{ccc} & G & \\ \varphi_1 \swarrow & & \searrow \varphi_2 \\ U_1 & \xrightarrow{h} & U_2 \end{array}$$

makes the isomorphism  $h$  “turn”  $\varphi_1$  into  $\varphi_2$ . For example, since  $(G/N, \pi_N)$  is a universal  $N$ -trivial group and (i)  $\ker \pi_N = N$  (not just  $N \subset \ker \pi_N$ ) and (ii)  $\pi_N(G) = G/N$ , every universal  $N$ -trivial group  $(U, \varphi)$  has similar properties:  $\ker \varphi = N$  and  $\varphi(G) = U$ . Indeed, letting  $h: (G/N, \pi_N) \rightarrow (U, \varphi)$  be the (unique) isomorphism between them, so  $h \circ \pi_N = \varphi$ , we have

$$\varphi(g) = 1 \implies h(\pi_N(g)) = 1 \implies \pi_N(g) = 1 \implies g \in N$$

since  $h$  is injective, so  $N \subset \ker \varphi \subset N$ . Thus  $\ker \varphi = N$ . Also

$$\varphi(G) = h(\pi_N(G)) = h(G/N) = U$$

since  $h$  and  $\pi_N$  are surjective. So  $\varphi: G \rightarrow U$  is onto with kernel  $N$ , just like  $\pi_N: G \rightarrow G/N$ .

This way of proving a universal  $N$ -trivial group  $(U, \varphi)$  has  $\ker \varphi = N$  and  $\varphi(G) = U$  uses our knowledge of these properties for the particular universal  $N$ -trivial group  $(G/N, \pi_N)$ . It turns out that these two properties can be shown *without* knowing a specific construction of a universal  $N$ -trivial group: it follows purely from reasoning based on the definition of a universal  $N$ -trivial group and its uniqueness up to unique isomorphism, as we now show.

**Theorem 2.9.** *If  $(U, \varphi)$  is a universal  $N$ -trivial group then  $\ker \varphi = N$ .*

*Proof.* By the definition of an  $N$ -trivial group,  $\varphi$  is trivial on  $N$ , so  $N \subset \ker \varphi$ . We want to get the reverse containment:  $\ker \varphi \subset N$ .

For every  $N$ -trivial group  $(\tilde{G}, f)$ , there is a (unique) homomorphism  $h: U \rightarrow \tilde{G}$  such that the following diagram commutes.

$$\begin{array}{ccc} & G & \\ \varphi \swarrow & & \searrow f \\ U & \xrightarrow{h} & \tilde{G} \end{array}$$

From this commutativity, if  $g \in \ker \varphi$  then  $f(g) = h(\varphi(g)) = h(1) = 1$  (all homomorphisms are trivial on the identity element), so  $g \in \ker f$ . Thus  $\ker \varphi \subset \ker f$  for every  $N$ -trivial group  $(\tilde{G}, f)$ . A particular  $N$ -trivial group is  $(G/N, \pi_N)$ , for which  $\ker \pi_N = N$ , so  $\ker \varphi \subset N$ . Thus  $\ker \varphi = N$ .  $\square$

While this proof used the quotient group  $G/N$  and reduction map  $\pi_N: G \rightarrow G/N$ , it did not rely on knowing  $(G/N, \pi_N)$  is a universal  $N$ -trivial group.

**Theorem 2.10.** *If  $(U, \varphi)$  is a universal  $N$ -trivial group then  $\varphi(G) = U$ .*

*Proof.* The image  $\varphi(G)$  is a subgroup of  $U$ . We want to show  $\varphi(G) = U$ . We will not use quotient groups in any way at all.

Since  $\varphi: G \rightarrow U$  is a homomorphism, so is  $G \rightarrow \varphi(G)$  also given by  $g \mapsto \varphi(g)$ . Call this map  $\varphi'$ , so  $\varphi': G \rightarrow \varphi(G)$  is  $\varphi$  with the target restricted to  $\varphi(G)$ . Since  $\varphi'$  is trivial on  $N$ ,  $(\varphi(G), \varphi')$  is an  $N$ -trivial group.

**Step 1.**  $(\varphi(G), \varphi')$  is a universal  $N$ -trivial group.

For each  $N$ -trivial group  $(\tilde{G}, f)$ , we want a unique morphism  $(\varphi(G), \varphi') \rightarrow (\tilde{G}, f)$ .

Existence of a morphism  $(\varphi(G), \varphi') \rightarrow (\tilde{G}, f)$ . Since  $(U, \varphi)$  is a universal  $N$ -trivial group there is a unique homomorphism  $U \xrightarrow{h} \tilde{G}$  making the following diagram commute.

$$\begin{array}{ccc} & G & \\ \varphi \swarrow & & \searrow f \\ U & \xrightarrow{h} & \tilde{G} \end{array}$$

The definition of  $\varphi(G)$  and  $\varphi': G \rightarrow \varphi(G)$  give us the following commutative diagram, where “incl.” is inclusion.

$$\begin{array}{ccc} & G & \\ \varphi' \swarrow & & \searrow \varphi \\ \varphi(G) & \xrightarrow{\text{incl.}} & U \end{array}$$

Stick these diagrams together to get the following commutative diagram.

$$\begin{array}{ccccc} & & G & & \\ & \varphi' \swarrow & \downarrow \varphi & \searrow f & \\ \varphi(G) & \xrightarrow{\text{incl.}} & U & \xrightarrow{h} & \tilde{G} \end{array}$$

Thus  $h \circ \text{incl.}$  is a morphism  $(\varphi(G), \varphi') \rightarrow (\tilde{G}, f)$  (Example 2.4).

Uniqueness of a morphism  $(\varphi(G), \varphi') \rightarrow (\tilde{G}, f)$ . If  $k$  is such a morphism then  $k(\varphi'(g)) = f(g)$ , so  $k(\varphi(g)) = f(g)$  for  $g \in G$ . The last formula shows  $k$  is determined as a function on  $\varphi(G)$ .

**Step 2.**  $\varphi(G) = U$ , so  $\varphi$  is surjective.

By Step 1,  $(\varphi(G), \varphi')$  is a universal  $N$ -trivial group, so Theorem 2.6 tells us that there is an isomorphism  $\psi: (\varphi(G), \varphi') \rightarrow (U, \varphi)$ , so the following diagram commutes.

$$\begin{array}{ccc} & G & \\ \varphi' \swarrow & & \searrow \varphi \\ \varphi(G) & \xrightarrow{\psi} & U \end{array}$$

Then  $\varphi = \psi \circ \varphi'$ , and  $\psi$  and  $\varphi'$  are surjective, so  $\varphi$  is surjective, which means  $U = \varphi(G)$ .  $\square$

### 3. THE ABELIANIZATION OF A GROUP

The commutator subgroup  $[G, G]$  of a group  $G$  is the subgroup generated by all commutators

$$[x, y] := xyx^{-1}y^{-1} \quad \text{for } x, y \in G.$$



Since  $[x, y]^{-1} = [y, x]$ ,  $[G, G]$  is the set of all *finite products of commutators*. (**Note:** in many groups  $G$ , each element of  $[G, G]$  is a commutator, but in general a product of commutators need not be a commutator, so  $[G, G]$  can be larger than the set of commutators.) What makes  $[G, G]$  important? We'll give two answers, as Theorems 3.2 and 3.4.

**Lemma 3.1.** *The subgroup  $[G, G]$  is normal in  $G$ ,*

*Proof.* In  $G$ , conjugation by a fixed element ( $h \mapsto ghg^{-1}$ ) is an automorphism, so it sends commutators to commutators and products of commutators to products of commutators:

$$\begin{aligned} g[x, y]g^{-1} &= g(xyx^{-1}y^{-1})g^{-1} \\ &= gxg^{-1} \cdot gyg^{-1} \cdot (gxg^{-1})^{-1} \cdot (gyg^{-1})^{-1} \\ &= [gxg^{-1}, gyg^{-1}] \end{aligned}$$

and therefore

$$\begin{aligned} g[x_1, y_1] \cdots [x_n, y_n]g^{-1} &= g[x_1, y_1]g^{-1} \cdots g[x_n, y_n]g^{-1} \\ &= [gx_1g^{-1}, gy_1g^{-1}] \cdots [gx_ng^{-1}, gy_ng^{-1}]. \end{aligned}$$

Therefore  $g[G, G]g^{-1} \subset [G, G]$  for all  $g \in G$ , so  $[G, G] \triangleleft G$ .  $\square$

**Theorem 3.2.** *The quotient group  $G/[G, G]$  is abelian, and  $G/N$  is abelian if and only if  $[G, G] \subset N$ .*

*Proof.* Commutators in  $G$  become trivial in  $G/[G, G]$ , so reducing the equation  $xy = [x, y]yx$  modulo  $[G, G]$  tells us  $\bar{x}\bar{y} = \bar{y}\bar{x}$  for all  $x$  and  $y$  in  $G$ , so  $G/[G, G]$  is abelian.

If  $G/N$  is abelian then for all  $x$  and  $y$  in  $G$ ,  $\bar{x}\bar{y} = \bar{y}\bar{x}$  in  $G/N$ , so  $\overline{[x, y]} = \bar{1}$  in  $G/N$ , or in other words  $[x, y] \in N$ . A subgroup containing all commutators must contain the subgroup they generate, so  $[G, G] \subset N$ . Another way to say this is that the homomorphism  $\pi_N: G \rightarrow G/N$  is trivial on commutators since commutators go to commutators by a homomorphism and  $G/N$  is abelian, so  $[x, y] \in \ker \pi_N = N$  for all  $x, y \in G$ . Thus  $[G, G] \subset N$ .  $\square$

Since abelian quotients  $G/N$  have  $[G, G] \subset N$ ,  $G/N \cong (G/[G, G])/(N/[G, G])$ , so  $G/[G, G]$  is an abelian quotient of  $G$  that explains all others (every quotient group of an abelian group is abelian). We can also say  $G/[G, G]$  is the largest abelian quotient of  $G$  since working modulo  $[G, G]$  trivializes the least amount of  $G$  to get an abelian quotient of  $G$ .

**Definition 3.3.** For a group  $G$ , its quotient  $G/[G, G]$  is called the *abelianization* of  $G$ .

Rather than explain the role of  $[G, G]$  in terms of its relation to all abelian quotient groups of  $G$ , the following theorem gives a relation to homomorphisms from  $G$  to all abelian groups.

**Theorem 3.4.** *If  $f: G \rightarrow A$  is a homomorphism from  $G$  to an abelian group  $A$  then there is a unique homomorphism  $\bar{f}: G/[G, G] \rightarrow A$  making the following diagram commute, where  $\pi: G \rightarrow G/[G, G]$  is the reduction map.*

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ & \searrow \pi & \nearrow \bar{f} \\ & G/[G, G] & \end{array}$$

*Proof.* If we have a group homomorphism  $f: G \rightarrow A$  where  $A$  is abelian, then  $f$  is trivial on commutators: in  $A$ :

$$f(xy x^{-1} y^{-1}) = f(x) f(y) f(x)^{-1} f(y)^{-1} = 1.$$

Therefore  $[x, y] \in \ker f$  for all  $x, y \in G$ , so  $[G, G] \subset \ker f$ . That means we get an induced homomorphism  $\bar{f}: G/[G, G] \rightarrow A$  where  $\bar{f}(g[G, G]) = f(g)$  for all  $g \in G$ . This is the unique homomorphism fitting into the commutative diagram in the theorem: if the diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ & \searrow \pi & \nearrow h \\ & G/[G, G] & \end{array}$$

commutes for some homomorphism  $h: G/[G, G] \rightarrow A$  then for each  $g \in G$ ,

$$h(\bar{g}) = h(\pi(g)) = f(g),$$

so  $h = \bar{f}$ . □

Rotating the commutative diagram in the statement of Theorem 3.4 to be

$$\begin{array}{ccc} & G & \\ \pi \swarrow & & \searrow f \\ G/[G, G] & \xrightarrow{\bar{f}} & A \end{array}$$

suggests thinking about the situation like this: reduction  $\pi: G \rightarrow G/[G, G]$  is one homomorphism from  $G$  to an abelian group and *all other* homomorphisms  $f: G \rightarrow A$  for abelian  $A$  are explained by composing  $\pi$  with homomorphisms  $\bar{f}$  from  $G/[G, G]$  to abelian groups: Theorem 3.4 shows  $f$  and  $\bar{f}$  determine each other.

To turn this into a universal mapping property, fix the group  $G$  and consider as objects of study all homomorphisms  $G \xrightarrow{f} A$  where  $A$  is abelian. We won't make up a name for these as before with “ $n$ -marked groups” and “ $N$ -trivial groups”.

**Example 3.5.** Reduction  $G \xrightarrow{\pi} G/[G, G]$  from  $G$  to its abelianization is such an object.

**Definition 3.6.** Given two such objects  $G \xrightarrow{f_1} A_1$  and  $G \xrightarrow{f_2} A_2$ , a *morphism* from the first to the second is a group homomorphism  $A_1 \xrightarrow{h} A_2$  such that the following diagram commutes.

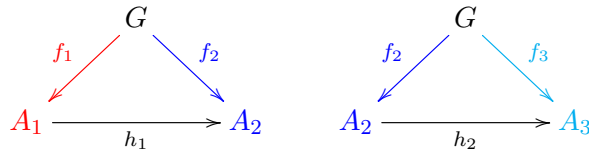
$$\begin{array}{ccc} & G & \\ f_1 \swarrow & & \searrow f_2 \\ A_1 & \xrightarrow{h} & A_2 \end{array}$$

We call  $h$  an *isomorphism* if it is an isomorphism from  $A_1$  to  $A_2$ .

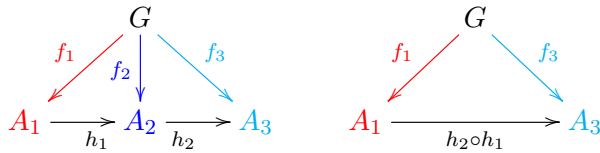
**Example 3.7.** For each  $G \xrightarrow{f} A$  we have the identity morphism of this object to itself.

$$\begin{array}{ccc} & G & \\ f \swarrow & & \searrow f \\ A & \xrightarrow{\text{id}} & A \end{array}$$

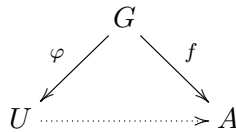
**Example 3.8.** For morphisms  $h_1$  and  $h_2$  as in the commutative diagrams below



the target  $G \xrightarrow{f_2} A_2$  of  $h_1$  is the source of  $h_2$ , so we can compose them by sticking the diagrams together to get a larger commutative diagram and then ignoring the middle arrow just as in Example 2.4.



**Definition 3.9.** Among all homomorphisms from  $G$  to abelian groups, say  $G \xrightarrow{\varphi} U$  is *universal* if for each  $G \xrightarrow{f} A$  there is a unique homomorphism  $U \rightarrow A$  making the following diagram commute,

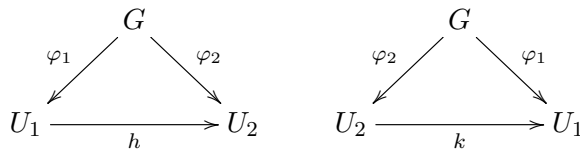


Equivalently, a universal object has a unique morphism to all other such objects.

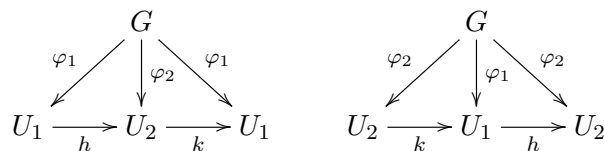
**Example 3.10.** Reduction  $G \xrightarrow{\pi} G/[G, G]$  to the abelianization of  $G$  is a universal object by Theorem 3.4. Rotate the diagram in that theorem to make it resemble the diagram above ( $U = G/[G, G]$ ,  $\varphi = \pi$ ). We say  $G/[G, G]$ , which really means  $G \xrightarrow{\pi} G/[G, G]$ , is “universal for homomorphisms from  $G$  to abelian groups.”

**Theorem 3.11.** If  $(U_1, \varphi_1)$  and  $(U_2, \varphi_2)$  are universal objects in the sense of Definition 3.9, then there is a unique morphism  $(U_1, \varphi_1) \rightarrow (U_2, \varphi_2)$  and it is an isomorphism.

*Proof.* This is the same proof as that of Theorem 2.6. Since  $(U_1, \varphi_1)$  and  $(U_2, \varphi_2)$  are universal, we have commutative diagrams



for unique group homomorphisms  $h$  and  $k$ . Compose  $h$  and  $k$  in both orders to get new diagrams.



Since the smaller triangles in each diagram commute, so do the big triangles, Removing the middle parts of the diagrams gives us the following commutative diagrams.

$$\begin{array}{ccc} & G & \\ \varphi_1 \swarrow & & \searrow \varphi_1 \\ U_1 & \xrightarrow{k \circ h} & U_1 \end{array} \qquad \begin{array}{ccc} & G & \\ \varphi_2 \swarrow & & \searrow \varphi_2 \\ U_2 & \xrightarrow{h \circ k} & U_2 \end{array}$$

Since  $(U_1, \varphi_1)$  is universal, only one homomorphism can appear where  $k \circ h$  does in the first commutative diagram. Since  $\text{id}_{U_1}$  fits,  $k \circ h = \text{id}_{U_1}$ . Similarly,  $h \circ k = \text{id}_{U_2}$  by the second commutative diagram and  $(U_2, \varphi_2)$  being universal. Therefore  $h$  and  $k$  are inverse isomorphisms between  $U_1$  and  $U_2$ .  $\square$

Since  $G \xrightarrow{\pi} G/[G, G]$  is a “universal homomorphism from  $G$  to abelian groups,” all other universal objects  $G \xrightarrow{\varphi} U$  are disguised versions of it by Theorem 3.11: there is an isomorphism between the groups  $G/[G, G]$  and  $U$  that turns  $\pi$  into  $\varphi$ . The next corollary is a consequence.

**Corollary 3.12.** *If  $G \xrightarrow{\varphi} U$  is universal for homomorphisms from  $G$  to abelian groups then  $\ker \varphi = [G, G]$  and  $\varphi(G) = U$ .*

*Proof.* We know  $G \xrightarrow{\pi} G/[G, G]$  is universal, so by Theorem 3.11 there is an isomorphism  $h: G/[G, G] \rightarrow U$  making the following diagram commute.

$$\begin{array}{ccc} & G & \\ \pi \swarrow & & \searrow \varphi \\ G/[G, G] & \xrightarrow{h} & U \end{array}$$

Then  $\varphi(g) = 1 \iff h(\pi(g)) = 1 \iff \pi(g) = 1$  since  $h$  is injective, so  $\ker \varphi = \ker \pi = [G, G]$ . Since  $h$  and  $\pi$  are surjective,  $\varphi = h \circ \pi$  is surjective, so  $\varphi(G) = U$ .  $\square$

**Remark 3.13.** This corollary can also be proved in the style of Theorems 2.9 and 2.10, making fuller use of the abstract universal mapping property and Theorem 3.11, never needing knowledge of any specific example of a universal object.

#### 4. DIRECT PRODUCT OF GROUPS

Fix groups  $G_1$  and  $G_2$ . We will describe a universal mapping property of the group  $G_1 \times G_2$  with componentwise operations. As in the previous examples, we need to think about  $G_1 \times G_2$  not by itself but equipped with extra mapping data. In this case, the extra data are the *projection homomorphisms*

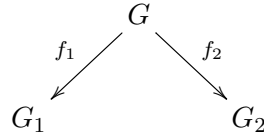
$$\text{pr}_1: G_1 \times G_2 \rightarrow G_1 \qquad \text{pr}_2: G_1 \times G_2 \rightarrow G_2$$

where  $\text{pr}_1(g_1, g_2) = g_1$  and  $\text{pr}_2(g_1, g_2) = g_2$ . These can be put together in a diagram:

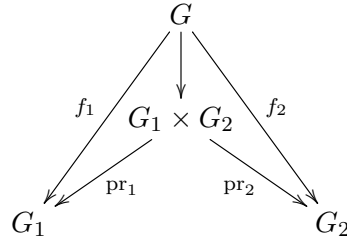
$$\begin{array}{ccc} & G_1 \times G_2 & \\ \text{pr}_1 \swarrow & & \searrow \text{pr}_2 \\ G_1 & & G_2 \end{array}$$

What is special about  $G_1 \times G_2$  together with its projection homomorphisms to  $G_1$  and  $G_2$  is that it “explains” pairs of homomorphisms from all groups to  $G_1$  and  $G_2$ .

**Theorem 4.1.** For every pair of homomorphisms  $f_1, f_2$  from an arbitrary group  $G$  to  $G_1$  and  $G_2$



set  $f: G \rightarrow G_1 \times G_2$  by  $f(g) = (f_1(g), f_2(g))$ . It is the unique homomorphism  $G \rightarrow G_1 \times G_2$  that makes the following big diagram commute.



*Proof.* Step 1. The mapping  $f$  in the theorem is a homomorphism.

This is a simple calculation: since  $f_1$  and  $f_2$  are homomorphisms, for each  $g \in G$

$$f(gg') = (f_1(gg'), f_2(gg')) = (f_1(g)f_1(g'), f_2(g)f_2(g')) = (f_1(g), f_2(g))(f_1(g'), f_2(g')),$$

which is  $f(g)f(g')$ .

Step 2. Using  $f$  as the homomorphism  $G \rightarrow G_1 \times G_2$ , the big diagram commutes.

By the defining formula  $f(g) = (f_1(g), f_2(g))$ , the first component function of  $f$  is  $f_1$  and the second component function of  $f$  is  $f_2$ . Thus  $\text{pr}_1 \circ f = f_1$  and  $\text{pr}_2 \circ f = f_2$ , which is what it means for the big diagram to commute.

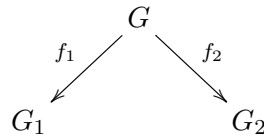
Step 3. A unique homomorphism  $h: G \rightarrow G_1 \times G_2$  makes the big diagram commute.

Suppose  $h: G \rightarrow G_1 \times G_2$  is a homomorphism making the big diagram commute. Write each value of  $h$  as  $h(g) = (a(g), b(g))$ , so

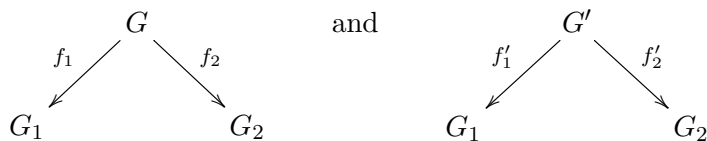
$$a(g) = \text{pr}_1(h(g)) = f_1(g) \quad \text{and} \quad b(g) = \text{pr}_2(h(g)) = f_2(g).$$

Thus  $h(g) = (f_1(g), f_2(g))$  for all  $g$ , so  $h$  must be the homomorphism we already met.  $\square$

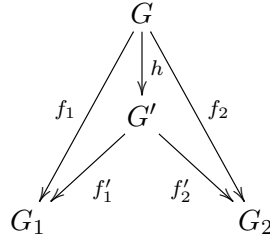
To formulate Theorem 4.1 as a universal mapping property for  $G_1 \times G_2$ , consider as new objects of interest all  $(G, f_1, f_2)$  where  $G$  is an arbitrary group and  $f_1: G \rightarrow G_1$  and  $f_2: G \rightarrow G_2$  are homomorphisms from  $G$  to fixed groups  $G_1$  and  $G_2$ . As a diagram,  $(G, f_1, f_2)$  looks like this.



**Definition 4.2.** Given any two such objects



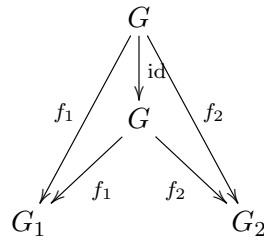
a *morphism* from  $(G, f_1, f_2)$  to  $(G', f'_1, f'_2)$  is a homomorphism  $h: G \rightarrow G'$  such that the following big diagram commutes.



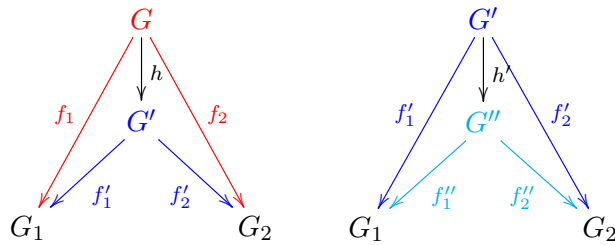
Call a morphism  $h$  an *isomorphism* if it is a group isomorphism from  $G$  to  $G'$ .

We are now viewing things vertically rather than horizontally: morphisms go “from top to bottom” rather than “from left to right”. Think of  $h: (G, f_1, f_2) \rightarrow (G', f'_1, f'_2)$  as turning  $G$  into  $G'$ ,  $f_1$  into  $f'_1$ , and  $f_2$  into  $f'_2$  by commutativity of the big diagram.

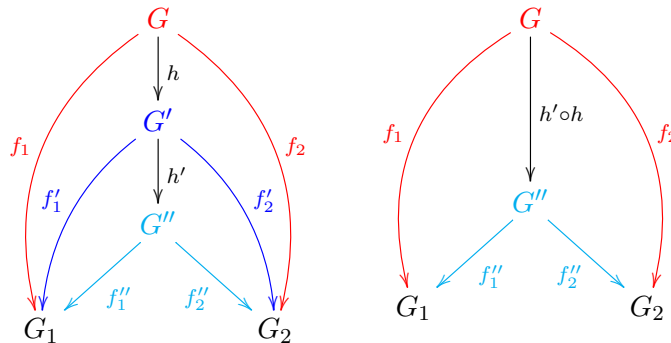
**Example 4.3.** For each triple  $(G, f_1, f_2)$ , the identity  $\text{id}: G \rightarrow G$  gives us a morphism from  $(G, f_1, f_2)$  to itself.



**Example 4.4.** Morphisms  $h: (G, f_1, f_2) \rightarrow (G', f'_1, f'_2)$  and  $h': (G', f'_1, f'_2) \rightarrow (G'', f''_1, f''_2)$  can be composed. The two commuting diagrams of group homomorphisms



can be placed on top of each other to get the large commuting diagram on the left, which becomes the one on the right after removing some parts linked to  $G'$  (it still commutes).



By the diagram on the right  $h' \circ h: (G, f_1, f_2) \rightarrow (G'', f_1'', f_2'')$  is a morphism.

Theorem 4.1 says for each  $(G, f_1, f_2)$  there is a unique morphism in the direction

$$(G, f_1, f_2) \rightarrow (G_1 \times G_2, \text{pr}_1, \text{pr}_2).$$

The previous universal properties we met (for cyclic groups, quotient groups, and abelianizations) have the universal object as a *source* of a unique morphism, but a direct product turns out to be the *target* of a unique morphism instead. That motivates the next definition.

**Definition 4.5.** An object  $(U, \varphi_1, \varphi_2)$  is called *universal* if every  $(G, f_1, f_2)$  admits a unique morphism to  $(U, \varphi_1, \varphi_2)$ .

**Example 4.6.** The triple  $(G_1 \times G_2, \text{pr}_1, \text{pr}_2)$  is universal by Theorem 4.1.

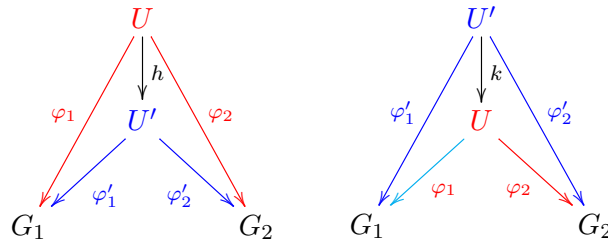
Let's think carefully about the directions of the arrows here. Why is it easier to write down a homomorphism  $G \rightarrow G_1 \times G_2$  rather than  $G_1 \times G_2 \rightarrow G$ ? The first kind of homomorphism only requires homomorphisms  $G \rightarrow G_1$  and  $G \rightarrow G_2$  and they don't have to be related in any way. On the other hand, if you want to write down a homomorphism  $G_1 \times G_2 \rightarrow G$  that goes out of a direct product, there are nontrivial constraints:  $(x, 1)$  and  $(1, y)$  commute in  $G_1 \times G_2$ , so a homomorphism out of  $G_1 \times G_2$  needs the images of  $G_1 \times \{1\}$  and  $\{1\} \times G_2$  to commute in  $G$ . If  $G$  is nonabelian, this is a serious constraint.<sup>1</sup> Trying to combine arbitrary homomorphisms  $G_1 \rightarrow G$  and  $G_2 \rightarrow G$  in some universal way to get a homomorphism out of some new group  $G_1 * G_2 \rightarrow G$  is related not to  $G_1 \times G_2$  but to the *free product* of  $G_1$  and  $G_2$ , which is complicated even when  $G_1$  and  $G_2$  are abelian, e.g. for  $\mathbf{Z}/2\mathbf{Z}$  and  $\mathbf{Z}/3\mathbf{Z}$ , their direct product is cyclic of order 6 while their free product is isomorphic to the infinite group  $\text{SL}_2(\mathbf{Z})/\{\pm I_2\}$ . The lesson is that for groups,

*it is easier to make a homomorphism to a direct product rather than from a direct product.*

Aside from reversing the direction of all the arrows, arguments from before about universal objects being “uniquely isomorphic” carry over to the setting of direct products. Let's check this.

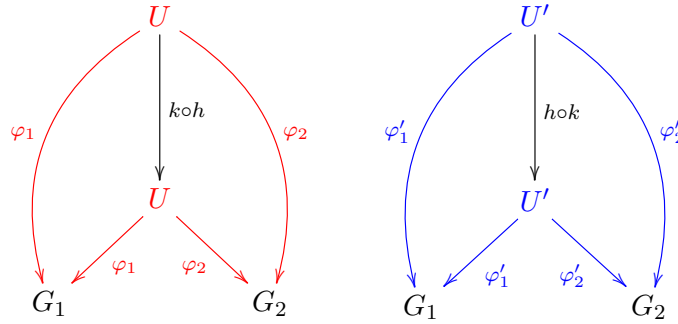
**Theorem 4.7.** If  $(U, \varphi_1, \varphi_2)$  and  $(U', \varphi'_1, \varphi'_2)$  are both universal then there is a unique morphism  $(U, \varphi_1, \varphi_2) \rightarrow (U', \varphi'_1, \varphi'_2)$  and it is an isomorphism.

*Proof.* There are unique homomorphisms  $h: U \rightarrow U'$ , and  $k: U' \rightarrow U$  fitting into the following commutative diagrams.



<sup>1</sup>If all the groups are abelian, there is no constraint at all and we get what would be called a direct sum rather than a direct product.

Composing these in both orders as in Example 4.4, we get commutative diagrams



Since  $\text{id}_U$  fits in the left diagram in place of  $h \circ k$  and  $\text{id}_{U'}$  fits in the right diagram in place of  $k \circ h$ , uniqueness of the homomorphism by universality implies  $k \circ h = \text{id}_U$  and  $h \circ k = \text{id}_{U'}$ . Therefore  $h$  and  $k$  are inverse isomorphisms between  $(U, \varphi_1, \varphi_2)$  and  $(U', \varphi'_1, \varphi'_2)$ .  $\square$

## 5. REVIEW AND INITIAL/FINAL OBJECTS

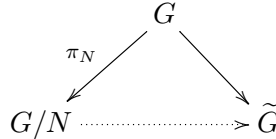
Let's review some constructions on groups characterized by a universal mapping property.

- (1) Cyclic group of order  $n$  for a positive integer  $n$ .

Among all groups  $G$  containing a chosen element  $\gamma$  such that  $\gamma^n = 1$ , a cyclic group  $C$  of order  $n$  and a chosen generator  $c$  “come first”: there is a unique homomorphism  $C \rightarrow G$  such that  $c \mapsto \gamma$ .

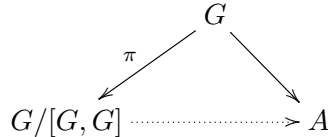
- (2) Quotient group  $G/N$  for a group  $G$  and normal subgroup  $N$ .

Among all homomorphisms  $G \rightarrow \tilde{G}$  that are trivial on  $N$ , the reduction map  $\pi_N: G \rightarrow G/N$  “comes first”: there is a unique homomorphism  $G/N \rightarrow \tilde{G}$  making the following diagram commute.



- (3) Abelianization of  $G$ .

Among all homomorphisms  $G \rightarrow A$  where  $A$  is abelian, the reduction map  $\pi: G \rightarrow G/[G, G]$  “comes first”: there is a unique homomorphism  $G/[G, G] \rightarrow A$  making the following diagram commute.

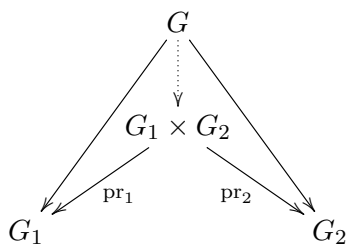


- (4) Direct product  $G_1 \times G_2$  of two groups  $G_1$  and  $G_2$ .

Among all  $(G, f_1, f_2)$  where  $G$  is a group and  $f_i: G \rightarrow G_i$  and  $f_2: G \rightarrow G_2$  are homomorphisms, the direct product  $G_1 \times G_2$  and its projections  $\text{pr}_1: G_1 \times G_2 \rightarrow G_1$  and  $\text{pr}_2: G_1 \times G_2 \rightarrow G_2$  “comes last”: there is a unique homomorphism  $G \rightarrow G_1 \times G_2$



making the following diagram commute.



In each of these settings we described a collection of objects and morphisms (maps) between them so that we can compose suitable morphisms (when the target object of the first morphism equals the source object of the second morphism) and we can make a particular construction of interest into an object that is “universal” in the sense of having a unique morphism to or from all other similar objects.

Each object has an identity morphism, and that is used to show two universal objects in each setting must have exactly one isomorphism between them: a universal object is “unique up to unique isomorphism” by a proof that is the same argument every time. These settings are called *categories*. A precise definition will not be given here (see textbooks for that), but the following examples of categories shows the wide scope of the concept.

- Groups and group homomorphisms
- Abelian groups and group homomorphisms
- Finite groups and group homomorphisms
- Rings and ring homomorphisms
- Commutative rings and ring homomorphisms
- Fields and field homomorphisms
- Vector spaces over a field  $F$  and  $F$ -linear maps
- Finite-dimensional vector spaces over a field  $F$  and linear maps
- Modules over a commutative ring  $R$  and  $R$ -linear maps
- Metric spaces and Lipschitz maps ( $d_Y(f(x), f(x')) \leq C d_X(x, x')$  for some  $C \geq 0$ )
- Topological spaces and continuous maps
- Smooth manifolds and smooth maps

None of these categories include our earlier examples. Here are the categories we created for them.

- For fixed  $n \geq 1$ , pairs  $(G, \gamma)$  where  $G$  is a group and  $\gamma \in G$  satisfies  $\gamma^n = 1$
- For fixed  $G$  and  $N \triangleleft G$ , pairs  $(\tilde{G}, f)$  where  $\tilde{G}$  is a group and  $f: G \rightarrow \tilde{G}$  is a group homomorphism that is trivial on  $N$
- For fixed  $G$ , pairs  $(A, f)$  where  $A$  is abelian and  $f: G \rightarrow A$  is a group homomorphism
- For fixed  $G_1$  and  $G_2$ , triples  $(G, f_1, f_2)$  where  $G$  is a group and  $f_1: G \rightarrow G_1$  and  $f_2: G \rightarrow G_2$  are group homomorphisms

In a category  $\mathcal{C}$ , each object  $A$  has an identity morphism  $\text{id}: A \rightarrow A$ . An *initial object* in  $\mathcal{C}$  is an object in  $\mathcal{C}$  that has a unique morphism *to* every other object in  $\mathcal{C}$ . A *final object* in  $\mathcal{C}$  is an object in  $\mathcal{C}$  that has a unique morphism *from* every other object in  $\mathcal{C}$ . What we have been calling a “universal mapping property” of some construction is really just an initial or final object in some category. Initial and final objects in a category don’t have to exist (examples are below), but if they do exist then they are “unique up to unique

isomorphism”: two initial objects have a unique morphism between them and it has to be isomorphism, and likewise for final objects.

What is an isomorphism of two objects in a category? This should generalize the idea of group isomorphisms, ring isomorphisms, and homeomorphisms of topological spaces. The definition we used earlier for a morphism to be called an isomorphism is not really the correct one. It works well in many algebraic settings, where bijective homomorphisms always have inverse maps that are homomorphisms. But in topology, a continuous bijection may not have a continuous inverse: continuity of the inverse is part of the definition of a homeomorphism (topological isomorphism). The correct definition of a morphism  $f: A \rightarrow B$  between two objects  $A$  and  $B$  in a category being an isomorphism is that there is an inverse morphism  $g: B \rightarrow A$ , meaning  $g \circ f = \text{id}_A$  and  $f \circ g = \text{id}_B$ .

Let’s look for initial and final objects in some categories.

- (1) Is there an initial object in the category of groups, *i.e.*, a group that admits a unique group homomorphism *to* all groups?

$$? \longrightarrow G$$

Yes: the trivial group. And obviously trivial groups are uniquely isomorphic.

You might wonder why  $\mathbf{Z}$  doesn’t fit the definition of an initial object in the category of groups. After all, for each group  $G$  and  $g \in G$ , there is a unique group homomorphism  $\mathbf{Z} \rightarrow G$  taking 1 to  $g$  by  $n \mapsto g^n$ . Isn’t that what initial objects are all about? No: we had to pick an element  $g$  first, and changing  $g$  changes the group homomorphism. Moreover, there is nothing group-theoretically special about 1 in  $\mathbf{Z}$  compared to  $-1$ .<sup>2</sup> In addition to a group homomorphism  $\mathbf{Z} \rightarrow G$  where  $n \mapsto g^n$  there is the group homomorphism  $\mathbf{Z} \rightarrow G$  where  $n \mapsto g^{-n}$ .

We could consider instead the category of “marked groups”: pairs  $(G, g)$  where  $g \in G$ , with a morphism of marked groups  $(G, g) \rightarrow (G', g')$  being a group homomorphism  $G \rightarrow G'$  such that  $g \mapsto g'$ . Is there an “initial” marked group?

$$? \longrightarrow (G, g)$$

Yes:  $(\mathbf{Z}, 1)$  fits. While a trivial group  $\{0\}$  is an initial object in the category of groups, the marked trivial group  $(\{0\}, 0)$  is *not* an initial object: there is a group homomorphism  $\{0\} \rightarrow \mathbf{Z}$ , but it does not send  $\{0\}$  to 1.

- (2) Is there a final group?

$$G \longrightarrow ?$$

The trivial group works here, and  $(\{0\}, 0)$  is a final object in the category of marked groups.

- (3) Is there an initial ring?

$$? \longrightarrow R$$

Yes: the ring  $\mathbf{Z}$  admits a unique ring homomorphism to every other ring: 1 in  $\mathbf{Z}$  has to go to 1 in  $R$  and everything else is then determined.

- (4) Is there a final ring?

$$R \longrightarrow ?$$

Yes: the zero ring  $\{0\}$  admits a unique ring homomorphism from every other ring. Note  $\mathbf{Z}$  is by no means a final ring, *e.g.*, there is no ring homomorphism  $\mathbf{Q} \rightarrow \mathbf{Z}$

<sup>2</sup>Of course there is a big difference between 1 and  $-1$  in  $\mathbf{Z}$  from the viewpoint of *ring theory*.

since it would be injective and there are no subfields of  $\mathbf{Z}$  (or it would have to map  $\mathbf{Q}^\times$  to  $\mathbf{Z}^\times$ , which is too small).

(5) Is there an initial field?

$$? \dashrightarrow F$$

No. But if we fix the characteristic of the field (0 or a prime  $p$ ) then there is an initial field:  $\mathbf{Q}$  for fields of characteristic 0 and  $\mathbf{Z}/p\mathbf{Z}$  for fields of characteristic  $p$ .

(6) Is there a final field?

$$F \dashrightarrow ?$$

No. Even if we fix the characteristic, there is still no final field. Field homomorphisms are always injective, so a final field would limit the possible cardinality of other fields, and there is no such restriction even if we fix the characteristic.

### 6. UNIVERSAL MAPPING PROPERTIES WITH RINGS

Having seen universal mapping properties at work in detail for several constructions in group theory, we'll treat examples in ring theory more concisely.

(1) **Quotient rings.**

For a commutative ring  $R$  and ideal  $I \subset R$ , the universal mapping property for  $R/I$  is analogous to that for quotient groups.

**Theorem 6.1.** *Let  $R$  be a commutative ring and  $I$  be an ideal. For every ring homomorphism  $f: R \rightarrow S$  such that  $f$  vanishes on  $I$ , there is a unique ring homomorphism  $\bar{f}: R/I \rightarrow S$  making the following diagram commute, where  $\pi_I: R \rightarrow R/I$  is the reduction map.*

$$\begin{array}{ccc} & R & \\ \pi_I \swarrow & & \searrow f \\ R/I & \xrightarrow{\bar{f}} & S \end{array}$$

As with quotient groups, this theorem is just as much about the reduction map  $R \xrightarrow{\pi_I} R/I$  as it is about the ring  $R/I$ . Both the ring  $R/I$  and the mapping  $\pi_I$  should be considered together.

To express this theorem as a universal mapping property, convert it into a statement about an initial object in a category by fixing the ring  $R$  and ideal  $I$  and defining the category of all pairs  $(S, f)$  where  $f: R \rightarrow S$  is a ring homomorphism that vanishes on  $I$ , with a morphism  $(S, f) \rightarrow (S', f')$  being a ring homomorphism  $h: S \rightarrow S'$  that makes the following diagram commute.

$$\begin{array}{ccc} & R & \\ f \swarrow & & \searrow f' \\ S & \xrightarrow{h} & S' \end{array}$$

(2) **Direct product of rings**

For two commutative rings  $R_1$  and  $R_2$ , the product ring  $R_1 \times R_2$  with componentwise operations admits projection homomorphisms  $\text{pr}_1: R_1 \times R_2 \rightarrow R_1$  and  $\text{pr}_2: R_1 \times R_2 \rightarrow R_2$ .

**Theorem 6.2.** *Let  $R_1$  and  $R_2$  be commutative rings. For every commutative ring  $R$  and pair of ring homomorphisms  $f_1: R \rightarrow R_1$  and  $f_2: R \rightarrow R_2$ , the mapping  $f: R \rightarrow R_1 \times R_2$  where  $f(r) = (f_1(r), f_2(r))$  is the unique ring homomorphism  $R \rightarrow R_1 \times R_2$  that makes the following diagram commute.*

$$\begin{array}{ccc}
 & R & \\
 f_1 \swarrow & \downarrow & \searrow f_2 \\
 & R_1 \times R_2 & \\
 \text{pr}_1 \swarrow & & \searrow \text{pr}_2 \\
 R_1 & & R_2
 \end{array}$$

This is a universal mapping property for product rings in the same sense as for product groups, by building a category with the product ring (and its projection maps) as a final object: the category of all triples  $(R, f_1, f_2)$  where  $f_1: R \rightarrow R_1$  and  $f_2: R \rightarrow R_2$  are ring homomorphisms, and a morphism  $(R, f_1, f_2) \rightarrow (R', f'_1, f'_2)$  is a ring homomorphism  $h: R \rightarrow R'$  that makes the following diagram commute.

$$\begin{array}{ccc}
 & R & \\
 f_1 \swarrow & \downarrow h & \searrow f_2 \\
 & R' & \\
 f'_1 \swarrow & & \searrow f'_2 \\
 R_1 & & R_2
 \end{array}$$

### (3) Fraction fields

An integral domain  $R$  has a fraction field  $F$ , which is all formal ratios  $a/b$  where  $a, b \in R$  with  $b \neq 0$ , and  $a/b = c/d$  when  $ad = bc$  in  $R$ . We embed  $R$  into  $F$  by sending  $a \in R$  to  $a/1$  in  $F$ . To avoid details of the construction of  $F$ , we'll compare  $F$  to other fields by emphasizing structural features in a universal mapping property.

For  $R = \mathbf{Z}$  and  $F = \mathbf{Q}$ , what is special about  $\mathbf{Q}$  is that it is a minimal field containing  $\mathbf{Z}$ . For a general integral domain  $R$ , its fraction field should be a minimal field containing  $R$ . That means every field  $K$  containing  $R$ , or more generally every field  $K$  that is the target of an injective ring homomorphism  $R \rightarrow K$ , contains the subfield generated by the image of  $R$ , and this should look like a copy of the fraction field of  $R$  within  $K$ . That motivates the next theorem about fraction fields.

**Theorem 6.3.** *Let  $R$  be an integral domain with fraction field  $F$  and embedding  $\iota: R \rightarrow F$  from the definition of fraction fields. For every field  $K$  and injective ring homomorphism  $f: R \rightarrow K$ , there is a unique ring homomorphism  $\varphi: F \rightarrow K$  that makes the following diagram commute.*

$$\begin{array}{ccc}
 & R & \\
 \iota \swarrow & & \searrow f \\
 F & \xrightarrow{\varphi} & K
 \end{array}$$

This makes the fraction field of  $R$  (and the embedding  $\iota: R \rightarrow F$  of  $R$  into its fraction field) an initial object of the following category: all pairs  $(K, f)$  where

$f: R \rightarrow K$  is an injective ring homomorphism<sup>3</sup> and a morphism  $(K, f) \rightarrow (K', f')$  is a field homomorphism  $h: K \rightarrow K'$  that makes the following diagram commute.

$$\begin{array}{ccc} & R & \\ f \swarrow & & \searrow f' \\ K & \xrightarrow{h} & K' \end{array}$$

## 7. UNIVERSAL MAPPING PROPERTIES WITH MODULES

Let  $R$  be a commutative ring. The important maps between  $R$ -modules are  $R$ -linear maps. Below we present theorems giving a context in which particular constructions of  $R$ -modules have a universal mapping property. We'll be more concise here than we were with rings; it is left to the reader to formulate the appropriate category in which the module construction becomes either an initial object or a final object.

### (1) Cyclic modules.

Every cyclic  $R$ -module is isomorphic to the  $R$ -module  $R/I$  for an ideal  $I$ , where  $I$  is the annihilator ideal of a generator of the module.

**Theorem 7.1.** *For an ideal  $I$  in  $R$ , let  $C = Rc$  be a cyclic  $R$ -module with a chosen generator  $c$  whose annihilator ideal  $\text{Ann}_R(c) = \{r \in R : rc = 0\}$  equals  $I$ .*

*For each  $R$ -module  $M$  containing an element  $m$  such that  $I \subset \text{Ann}_R(m)$ , there is a unique  $R$ -linear map  $f: C \rightarrow M$  such that  $f(c) = m$ .*

### (2) Quotient modules.

**Theorem 7.2.** *Let  $M$  be an  $R$ -module and  $N$  be a submodule. For every  $R$ -module  $P$  and  $R$ -linear map  $f: M \rightarrow P$  such that  $f$  vanishes on  $N$ , there is a unique  $R$ -linear map  $\bar{f}: M/N \rightarrow P$  making the following diagram commute, where  $\pi_N: M \rightarrow M/N$  is the reduction map.*

$$\begin{array}{ccc} & M & \\ \pi_N \swarrow & & \searrow f \\ M/N & \xrightarrow{\bar{f}} & P \end{array}$$

### (3) Direct product of $R$ -modules.

Our discussion of direct products of groups and rings used only two groups and two rings. We'll allow an arbitrary collection of factors in a direct product module

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i\}.$$

This makes it easier to see a difference with direct sums (coming up next).

As with most product constructions, what is important are the projection maps  $\text{pr}_j: \prod_{i \in I} M_i \rightarrow M_j$  for each  $j \in I$ , which are all  $R$ -linear. Different projection maps don't have anything to do with each other, so the next theorem uses a separate commutative diagram for each  $\text{pr}_j$ , rather than one diagram involving all of them as we did with a product of two groups and two rings.

<sup>3</sup>Not all homomorphisms from an integral domain to a field have to be injective: consider  $\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  for primes  $p$ .

**Theorem 7.3.** For each  $R$ -module  $N$  and  $R$ -linear maps  $f_i: N \rightarrow M_i$  for  $i \in I$ , there is a unique  $R$ -linear map  $f: N \rightarrow \prod_{i \in I} M_i$  making the following diagrams commute for all  $j$ .

$$\begin{array}{ccc} N & \xrightarrow{f} & \prod_{i \in I} M_i \\ & \searrow f_j & \swarrow \text{pr}_j \\ & & M_j \end{array}$$

This  $f$  is the function where  $f(n) = (f_i(n))_{i \in I}$  for all  $n \in N$ .

(4) **Direct sum of  $R$ -modules.**

In a direct sum

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i, \text{ all but finitely many } m_i = 0\},$$

each element is built from finitely many pieces (its nonzero components). We can embed  $M_i$  into the direct sum using the  $i$ th component (and zero elsewhere), which makes the  $M_i$ 's submodules of the direct sum and they span it (using finite  $R$ -linear combinations). While direct product modules have projection maps *out*, direct sum modules have embedding maps *in*:  $\iota_j: M_j \rightarrow \bigoplus_{i \in I} M_i$ .

**Theorem 7.4.** For each  $R$ -module  $N$  and  $R$ -linear maps  $f_i: M_i \rightarrow N$  for  $i \in I$ , there is a unique  $R$ -linear map  $f: \bigoplus_{i \in I} M_i \rightarrow N$  making the following diagrams commute for all  $j$ .

$$\begin{array}{ccc} & M_j & \\ \iota_j \swarrow & & \searrow f_j \\ \bigoplus_{i \in I} M_i & \xrightarrow{f} & N \end{array}$$

This  $f$  is the function where  $f(\sum_i m_i) = \sum_i f_i(m_i)$  for all  $\sum_i m_i \in \bigoplus_{i \in I} M_i$ .

Comparing this to Theorem 7.3, the universal mapping properties of direct products and direct sums turn into one another by formally reversing all the arrows: maps  $N \rightarrow M_i$  become  $M_i \rightarrow N$ ,  $f: N \rightarrow \prod_{i \in I} M_i$  becomes  $f: \bigoplus_{i \in I} M_i \rightarrow N$ , and  $\text{pr}_j: \prod_{i \in I} M_i \rightarrow M_j$  becomes  $\iota_j: M_j \rightarrow \bigoplus_{i \in I} M_i$ .

(5) **Free  $R$ -modules.**

For a set  $X$ , the embedding  $i: X \hookrightarrow F_R(X)$  to the free  $R$ -module on  $X$  by  $x \mapsto \delta_x$  is one function from  $X$  to an  $R$ -module. It explains all other functions from  $X$  to  $R$ -modules by the following theorem.

**Theorem 7.5.** Let  $X$  be a set. For each  $R$ -module  $M$  and function  $f: X \rightarrow M$ , there is a unique  $R$ -linear map  $F_R(X) \rightarrow M$  making the following diagram commute.

$$\begin{array}{ccc} & X & \\ \iota \swarrow & & \searrow f \\ F_R(X) & \longrightarrow & M \end{array}$$

One reason for naming  $F_R(X)$  a “free”  $R$ -module on  $X$  is that it is an  $R$ -module containing  $X$  (or at least a subset that looks like  $X$ ) as a basis, so the elements

of  $X$  are free of  $R$ -linear relations when viewed in  $F_R(X)$ . Theorem 7.5 provides another reason for the label “free”: to write down an  $R$ -linear function from  $F_R(X)$  to an  $R$ -module  $M$ , we need to send the elements of  $X$  somewhere in  $M$  and there is complete freedom in doing this, since each function  $X \rightarrow M$  uniquely extends to an  $R$ -linear function  $F_R(X) \rightarrow M$ .

When  $X$  is a finite set of size  $n$ , so  $F_R(X) \cong R^n$ , the theorem simply says each function from a basis of  $R^n$  to an  $R$ -module  $M$  extends uniquely to a linear function  $R^n \rightarrow M$ .

APPENDIX A. SOME UNIVERSAL MAPPING PROPERTIES OUTSIDE OF ALGEBRA

We briefly present here universal mapping properties for the product topology, the quotient topology, and the completion of a metric space.

(1) **Product topology.**

For topological spaces  $X_i$ , the product topology on

$$\prod_{i \in I} X_i = \{(x_i)_{i \in I} : x_i \in X_i\}$$

makes all projection maps  $\text{pr}_j: \prod_{i \in I} X_i \rightarrow X_j$  continuous and it is the smallest such topology on the product space. That could be considered a nice aspect of the product topology: projections are important, so making them continuous should be the minimal requirement we have for a topology put on  $\prod_{i \in I} X_i$ . The following theorem promotes continuity of the projection maps to a universal mapping property for  $\prod_{i \in I} X_i$  and its projections.

**Theorem A.1.** *For each topological space  $Y$  and continuous maps  $f_i: Y \rightarrow X_i$  for  $i \in I$ , there is a unique continuous map  $f: Y \rightarrow \prod_{i \in I} X_i$ , where  $\prod_{i \in I} X_i$  has the product topology, that makes the following diagram commute for every  $j$ .*

$$\begin{array}{ccc} Y & \xrightarrow{f} & \prod_{i \in I} X_i \\ & \searrow f_j & \swarrow \text{pr}_j \\ & X_j & \end{array}$$

*This  $f$  is the function where  $f(y) = (f_i(y))_{i \in I}$  for each  $y \in Y$ .*

(2) **Quotient topology.**

For an equivalence relation  $\sim$  on a topological space  $X$ , we have the canonical surjective mapping  $\pi: X \rightarrow X/\sim$  that sends each  $x \in X$  to its equivalence class  $[x]$  with respect to  $\sim$ . The quotient topology on  $X/\sim$ , where a subset  $U$  of  $X/\sim$  is called open if and only if  $\pi^{-1}(U)$  is open in  $X$ , is the smallest topology on  $X/\sim$  that makes  $\pi: X \rightarrow X/\sim$  continuous. That  $\pi$  is continuous on  $X$  and constant on  $\sim$ -equivalence classes leads to the following universal mapping property for the quotient space  $X/\sim$  and  $\pi$ .

**Theorem A.2.** *Let  $X$  be a topological space and  $\sim$  be an equivalence relation on  $X$ . For each topological space  $Y$  and continuous function  $f: X \rightarrow Y$  such that  $x \sim x' \Rightarrow f(x) = f(x')$  for all  $x$  and  $x'$  in  $X$ , there is a unique continuous map  $\bar{f}: X/\sim \rightarrow Y$ ,*

where  $X/\sim$  has the quotient topology, that makes the following diagram commute.

$$\begin{array}{ccc} & X & \\ \pi \swarrow & & \searrow f \\ X/\sim & \xrightarrow{\bar{f}} & Y \end{array}$$

This  $\bar{f}$  is the function where  $\bar{f}([x]) = f(x)$  for each  $x \in X$ .

(3) **Completion of a metric space.**

The completion of a metric space  $(X, d_X)$  is a complete metric space  $(\widehat{X}, \widehat{d}_X)$  into which  $X$  embeds isometrically (preserving distances) with a dense image. The point of having a dense image is that it makes the closure of  $X$  in  $\widehat{X}$  equal to  $\widehat{X}$ . For instance the completion of  $\mathbf{Q}$  with respect to the metric  $d(r, s) = |r - s|$  is  $\mathbf{R}$ , not  $\mathbf{C}$ , even though  $\mathbf{C}$  is a complete metric space into which the metric space  $\mathbf{Q}$  has an isometric embedding.

There are multiple ways to show a metric space has a completion.<sup>4</sup> Here is a universal mapping property for completions, which is applicable no matter what method is used to show the completion exists.

**Theorem A.3.** *Let  $(X, d_X)$  be a metric space. For each complete metric space  $(C, d_C)$  and isometry  $f: X \rightarrow C$ , there is a unique isometry  $\widehat{f}: \widehat{X} \rightarrow C$  that makes the following diagram commute, where  $i_X: X \rightarrow \widehat{X}$  is an isometric embedding of  $X$  into a completion of  $X$ .*

$$\begin{array}{ccc} & (X, d_X) & \\ i_X \swarrow & & \searrow f \\ (\widehat{X}, \widehat{d}_X) & \xrightarrow{\widehat{f}} & (C, d_C) \end{array}$$

The commutativity of this diagram says a completion of  $X$  maps uniquely to all other complete metric spaces  $C$  in which there is an isometric embedding of  $X$ .

---

<sup>4</sup>See the appendix of <https://kconrad.math.uconn.edu/blurbs/analysis/metricspaces.pdf>.