

# The Canonical Factorization of a Homomorphism



# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.**

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature,

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ ,

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$  ( $\subseteq B$ ), then we must have

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$  ( $\subseteq B$ ), then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$  ( $\subseteq B$ ), then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h)$

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$  ( $\subseteq B$ ), then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h)$  ( $\subseteq B$ )

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ .

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$  ( $\subseteq B$ ), then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h)$  ( $\subseteq B$ ) must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of**  $\mathbb{B}$ .

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$

# Image

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$  is a (i) subset of  $B$

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$  is a (i) subset of  $B$  that is (ii) **closed under the operations of the signature**,

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$  is a (i) subset of  $B$  that is (ii) **closed under the operations of the signature**, equipped with operations that are the restrictions of the operations from  $\mathbb{B}$ .

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$  is a (i) subset of  $B$  that is (ii) **closed under the operations of the signature**, equipped with operations that are the restrictions of the operations from  $\mathbb{B}$ .

**Fact 2.**

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h) (\subseteq B)$ , then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h) (\subseteq B)$  must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$  is a (i) subset of  $B$  that is (ii) **closed under the operations of the signature**, equipped with operations that are the restrictions of the operations from  $\mathbb{B}$ .

**Fact 2.** With the above definition, the inclusion map  $\iota: \text{im}(h) \rightarrow \mathbb{B}: b \mapsto b$  is a homomorphism.

Let  $h: \mathbb{A} \rightarrow \mathbb{B}$  be a homomorphism.

**Fact 1.** There is a unique algebra structure on  $\text{im}(h)$  that makes  $h: \mathbb{A} \rightarrow \text{im}(h)$  a homomorphism.

If  $f(x_1, \dots, x_n)$  is an operation of the signature, and  $b_1, \dots, b_n \in \text{im}(h)$  ( $\subseteq B$ ), then we must have

$$f^{\text{im}(h)}(b_1, \dots, b_n) = f^{\mathbb{B}}(b_1, \dots, b_n).$$

That is, the definition of  $f$  on  $\text{im}(h)$  ( $\subseteq B$ ) must be the restriction of the definition of  $f$  on  $\mathbb{B}$ . This forces  $\text{im}(h)$  to be **closed under the operations of  $\mathbb{B}$** . We therefore choose the definition of “subalgebra”, so that a **subalgebra** of  $\mathbb{B}$  is a (i) subset of  $B$  that is (ii) **closed under the operations of the signature**, equipped with operations that are the restrictions of the operations from  $\mathbb{B}$ .

**Fact 2.** With the above definition, the inclusion map  $\iota: \text{im}(h) \rightarrow \mathbb{B}: b \mapsto b$  is a homomorphism.



## Fact 3.

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$[a_1] = [c_1]$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{aligned} [a_1] &= [c_1] \\ [a_2] &= [c_2] \end{aligned}$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$[a_1] = [c_1]$$

$$[a_2] = [c_2]$$

$$\vdots$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$[a_1] = [c_1]$$

$$[a_2] = [c_2]$$

$$\vdots$$

$$[a_n] = [c_n]$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{aligned} [a_1] &= [c_1] \\ [a_2] &= [c_2] \\ &\vdots \\ [a_n] &= [c_n] \\ &\implies \end{aligned}$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{aligned} [a_1] &= [c_1] \\ [a_2] &= [c_2] \\ &\vdots \\ [a_n] &= [c_n] \\ &\implies \\ [f^{\mathbb{A}}(a_1, \dots, a_n)] &= [f^{\mathbb{A}}(c_1, \dots, c_n)] \end{aligned}$$

**Fact 3.** There is a unique algebra structure on  $\text{coim}(h)$  that makes the natural map  $\nu: \mathbb{A} \rightarrow \text{coim}(h): a \mapsto [a]$  a homomorphism.

The only possible choice is

$$f^{\text{coim}(h)}([a_1], \dots, [a_n]) = [f^{\mathbb{A}}(a_1, \dots, a_n)].$$

(Check!)  $f^{\text{coim}(h)}$  will be **well-defined** iff that the following implication holds:  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{aligned} [a_1] &= [c_1] \\ [a_2] &= [c_2] \\ &\vdots \\ [a_n] &= [c_n] \\ &\implies \\ [f^{\mathbb{A}}(a_1, \dots, a_n)] &= [f^{\mathbb{A}}(c_1, \dots, c_n)] \end{aligned}$$

# Coimage versus kernel

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ )

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.**

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ .

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$a_1 \equiv c_1 \quad (\text{mod } \ker(h))$$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{array}{ll} a_1 & \equiv c_1 & (\text{mod } \ker(h)) \\ a_2 & \equiv c_2 & (\text{mod } \ker(h)) \end{array}$$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{array}{lll} a_1 & \equiv & c_1 & (\text{mod } \ker(h)) \\ a_2 & \equiv & c_2 & (\text{mod } \ker(h)) \\ & \vdots & & \end{array}$$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{array}{lll} a_1 & \equiv & c_1 & (\text{mod } \ker(h)) \\ a_2 & \equiv & c_2 & (\text{mod } \ker(h)) \\ & \vdots & & \\ a_n & \equiv & c_n & (\text{mod } \ker(h)) \end{array}$$

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{array}{rcl} a_1 & \equiv & c_1 & (\text{mod } \ker(h)) \\ a_2 & \equiv & c_2 & (\text{mod } \ker(h)) \\ & \vdots & & \\ a_n & \equiv & c_n & (\text{mod } \ker(h)) \end{array}$$

---

# Coimage versus kernel

The data of Fact 3 can be expressed in terms of the **coimage** of  $h$  (which is a **partition** of  $\text{dom}(h)$ ) or in terms of the **kernel** of  $h$  (which is the associated **equivalence relation**).

**Definition.** The **kernel** of a function  $h: A \rightarrow B$  is the equivalence relation

$$\ker(h) = \{(a, c) \in A^2 \mid h(a) = h(c)\}.$$

The set of equivalence classes of  $\ker(h)$  is  $A/\ker(h) = \text{coim}(h)$ . The condition for an operation to be well-defined on  $A/\ker(h)$  is  $(\forall \mathbf{a} \in A^n)(\forall \mathbf{c} \in A^n)$

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } \ker(h)) \\ a_2 & \equiv & c_2 \quad (\text{mod } \ker(h)) \\ & \vdots & \\ a_n & \equiv & c_n \quad (\text{mod } \ker(h)) \\ \hline f^{\mathbb{A}}(a_1, \dots, a_n) & \equiv & f^{\mathbb{A}}(c_1, \dots, c_n) \quad (\text{mod } \ker(h)) \end{array}$$



# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, {}^{-1}, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism.

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

## Example.

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot,^{-1}, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

## Example.

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -^1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers)

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -^1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers).

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, {}^{-1}, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, {}^{-1}, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$a_1 \equiv c_1 \quad (\text{mod } P)$$

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{aligned} a_1 &\equiv c_1 && (\text{mod } P) \\ a_2 &\equiv c_2 && (\text{mod } P) \end{aligned}$$

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } P) \\ a_2 & \equiv & c_2 \quad (\text{mod } P) \\ \hline \end{array}$$

The kernel of an algebra homomorphism is called a **congruence**.

**Example.**

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } P) \\ a_2 & \equiv & c_2 \quad (\text{mod } P) \\ \hline a_1 + a_2 & \equiv & c_1 + c_2 \quad (\text{mod } P) \end{array}$$

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

## Example.

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } P) \\ a_2 & \equiv & c_2 \quad (\text{mod } P) \\ \hline a_1 + a_2 & \equiv & c_1 + c_2 \quad (\text{mod } P) \\ \hline \end{array}$$

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

## Example.

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } P) \\ a_2 & \equiv & c_2 \quad (\text{mod } P) \\ \hline a_1 + a_2 & \equiv & c_1 + c_2 \quad (\text{mod } P) \\ \hline -a_1 & \equiv & -c_1 \quad (\text{mod } P) \end{array}$$

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

## Example.

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } P) \\ a_2 & \equiv & c_2 \quad (\text{mod } P) \\ \hline a_1 + a_2 & \equiv & c_1 + c_2 \quad (\text{mod } P) \\ \hline -a_1 & \equiv & -c_1 \quad (\text{mod } P) \\ \hline \end{array}$$

# Congruences

The kernel of an algebra homomorphism is called a **congruence**.

## Example.

The function  $h: \langle \mathbb{Z}; +, -, 0 \rangle \rightarrow \langle \{1, -1\}; \cdot, -1, 1 \rangle: 2m \mapsto 1, 2n + 1 \mapsto -1$  is a group homomorphism. Its kernel is the equivalence relation  $P$  on  $\mathbb{Z}$  that has two equivalence classes:  $2\mathbb{Z}$  (the even integers) and  $1 + 2\mathbb{Z}$  (the odd integers). The fact that this equivalence relation is a congruence follows from:

$$\begin{array}{rcl} a_1 & \equiv & c_1 \quad (\text{mod } P) \\ a_2 & \equiv & c_2 \quad (\text{mod } P) \\ \hline a_1 + a_2 & \equiv & c_1 + c_2 \quad (\text{mod } P) \\ \hline -a_1 & \equiv & -c_1 \quad (\text{mod } P) \\ \hline 0 & \equiv & 0 \quad (\text{mod } P) \end{array}$$

# The Induced Map

# The Induced Map

**Fact 4.**

# The Induced Map

**Fact 4.** The induced map

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.*

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection.

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism,

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

$$\bar{h}(f^{\text{coim}(h)}([a_1], \dots, [a_n])) = \bar{h}([f^{\mathbb{A}}(a_1, \dots, a_n)])$$

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

$$\begin{aligned} \bar{h}(f^{\text{coim}(h)}([a_1], \dots, [a_n])) &= \bar{h}([f^{\mathbb{A}}(a_1, \dots, a_n)]) \\ &= h(f^{\mathbb{A}}(a_1, \dots, a_n)) \end{aligned}$$

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

$$\begin{aligned}\bar{h}(f^{\text{coim}(h)}([a_1], \dots, [a_n])) &= \bar{h}([f^{\mathbb{A}}(a_1, \dots, a_n)]) \\ &= h(f^{\mathbb{A}}(a_1, \dots, a_n)) \\ &= f^{\mathbb{B}}(h(a_1), \dots, h(a_n))\end{aligned}$$

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

$$\begin{aligned} \bar{h}(f^{\text{coim}(h)}([a_1], \dots, [a_n])) &= \bar{h}([f^{\text{A}}(a_1, \dots, a_n)]) \\ &= h(f^{\text{A}}(a_1, \dots, a_n)) \\ &= f^{\text{B}}(h(a_1), \dots, h(a_n)) \\ &= f^{\text{im}(h)}(h(a_1), \dots, h(a_n)) \end{aligned}$$

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

$$\begin{aligned} \bar{h}(f^{\text{coim}(h)}([a_1], \dots, [a_n])) &= \bar{h}([f^{\text{A}}(a_1, \dots, a_n)]) \\ &= h(f^{\text{A}}(a_1, \dots, a_n)) \\ &= f^{\text{B}}(h(a_1), \dots, h(a_n)) \\ &= f^{\text{im}(h)}(h(a_1), \dots, h(a_n)) \\ &= f^{\text{im}(h)}(\bar{h}([a_1]), \dots, \bar{h}([a_n])). \end{aligned}$$

# The Induced Map

**Fact 4.** The induced map

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h): [a] \mapsto h(a)$$

is an isomorphism.

*Proof.* The induced map is always a bijection. To see that it is a homomorphism, compute that

$$\begin{aligned} \bar{h}(f^{\text{coim}(h)}([a_1], \dots, [a_n])) &= \bar{h}([f^{\text{A}}(a_1, \dots, a_n)]) \\ &= h(f^{\text{A}}(a_1, \dots, a_n)) \\ &= f^{\text{B}}(h(a_1), \dots, h(a_n)) \\ &= f^{\text{im}(h)}(h(a_1), \dots, h(a_n)) \\ &= f^{\text{im}(h)}(\bar{h}([a_1]), \dots, \bar{h}([a_n])). \end{aligned}$$

# The Induced Map, 2

# The Induced Map, 2

We complete the argument with an important result:

# The Induced Map, 2

We complete the argument with an important result:

**Theorem.**

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.*

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism.

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ;

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations.

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

## The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

$$hh^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq hf^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n))$$

# The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

$$\begin{aligned} hh^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) &\neq hf^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(hh^{-1}(b_1), \dots, hh^{-1}(b_n)) \end{aligned}$$

# The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

$$\begin{aligned} hh^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) &\neq hf^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(hh^{-1}(b_1), \dots, hh^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(b_1, \dots, b_n). \end{aligned}$$

# The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

$$\begin{aligned} hh^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) &\neq hf^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(hh^{-1}(b_1), \dots, hh^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(b_1, \dots, b_n). \end{aligned}$$

# The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

$$\begin{aligned} hh^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) &\neq hf^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(hh^{-1}(b_1), \dots, hh^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(b_1, \dots, b_n). \end{aligned}$$

The last line is false, so we have obtained a contradiction.

# The Induced Map, 2

We complete the argument with an important result:

**Theorem.** A bijective algebra homomorphism is an isomorphism.

*Proof.* Assume that  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a bijective homomorphism. The inverse function  $h^{-1}$  is a map from  $B$  to  $A$ ; we must explain why it preserves the operations. We shall assume that it does not and derive a contradiction.

Assume that

$$h^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) \neq f^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)).$$

Apply the injective function  $h$  to these two distinct elements. The results should be distinct:

$$\begin{aligned} hh^{-1}(f^{\mathbb{B}}(b_1, \dots, b_n)) &\neq hf^{\mathbb{A}}(h^{-1}(b_1), \dots, h^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(hh^{-1}(b_1), \dots, hh^{-1}(b_n)) \\ f^{\mathbb{B}}(b_1, \dots, b_n) &\neq f^{\mathbb{B}}(b_1, \dots, b_n). \end{aligned}$$

The last line is false, so we have obtained a contradiction.  $\square$

# The First Isomorphism Theorem

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.**

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.** If  $h: \mathbb{A} \rightarrow \mathbb{B}$  is an algebra homomorphism, then

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.** If  $h: \mathbb{A} \rightarrow \mathbb{B}$  is an algebra homomorphism, then

$$\bar{h}: \mathbb{A} / \ker(h) \rightarrow \text{im}(h)$$

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.** If  $h: \mathbb{A} \rightarrow \mathbb{B}$  is an algebra homomorphism, then

$$\bar{h}: \mathbb{A} / \ker(h) \rightarrow \text{im}(h)$$

is an isomorphism.

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.** If  $h: \mathbb{A} \rightarrow \mathbb{B}$  is an algebra homomorphism, then

$$\bar{h}: \mathbb{A}/\ker(h) \rightarrow \text{im}(h)$$

is an isomorphism.

The displayed line in the First Isomorphism Theorem may be written

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.** If  $h: \mathbb{A} \rightarrow \mathbb{B}$  is an algebra homomorphism, then

$$\bar{h}: \mathbb{A}/\ker(h) \rightarrow \text{im}(h)$$

is an isomorphism.

The displayed line in the First Isomorphism Theorem may be written

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h)$$

# The First Isomorphism Theorem

The fact that the induced map associated to a homomorphism is an isomorphism is called the

**The First Isomorphism Theorem.** If  $h: \mathbb{A} \rightarrow \mathbb{B}$  is an algebra homomorphism, then

$$\bar{h}: \mathbb{A} / \ker(h) \rightarrow \text{im}(h)$$

is an isomorphism.

The displayed line in the First Isomorphism Theorem may be written

$$\bar{h}: \text{coim}(h) \rightarrow \text{im}(h)$$

instead, but the form I used first is the more common form.

# The Canonical Factorization of a Homomorphism

# The Canonical Factorization of a Homomorphism

The canonical factorization of a **function**  $h: A \rightarrow B$  is  $h = \iota \circ \bar{h} \circ \nu$ .

# The Canonical Factorization of a Homomorphism

The canonical factorization of a **function**  $h: A \rightarrow B$  is  $h = \iota \circ \bar{h} \circ \nu$ . Each of these composition factors is a set-function.

# The Canonical Factorization of a Homomorphism

The canonical factorization of a **function**  $h: A \rightarrow B$  is  $h = \iota \circ \bar{h} \circ \nu$ . Each of these composition factors is a set-function. These slides explain why, if  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a **homomorphism of algebras**, then  $\text{im}(h)$  and  $\text{coim}(h)$  can be equipped with unique algebra structure so that  $h = \iota \circ \bar{h} \circ \nu$  is a factorization of  $h$  into **algebra homomorphisms**.

# The Canonical Factorization of a Homomorphism

The canonical factorization of a **function**  $h: A \rightarrow B$  is  $h = \iota \circ \bar{h} \circ \nu$ . Each of these composition factors is a set-function. These slides explain why, if  $h: \mathbb{A} \rightarrow \mathbb{B}$  is a **homomorphism of algebras**, then  $\text{im}(h)$  and  $\text{coim}(h)$  can be equipped with unique algebra structure so that  $h = \iota \circ \bar{h} \circ \nu$  is a factorization of  $h$  into **algebra homomorphisms**.