SAMPLE EXERCISE 1

MONDAY JANUARY 24, 2011

ABSTRACT. This is a sample solution to one of the in-class exercises.

1. Exercise

Let $(S, *)$ and $(T, \perp)$ be two binary structures. Let

$$f : (S, *) \to (T, \perp)$$

be a morphism of binary structures. Show that f is an isomorphism of binary structures if and only if it is both injective and surjective.

2. Solution

Recall [1] that a morphism of binary structures

$$f : (S, *) \to (T, \perp)$$

consists of a map of sets [2]

$$F : S \to T$$

such that for all $s_1, s_2 \in S$,

$$F(s_1 * s_2) = F(s_1) \perp F(s_2). \tag{2.1}$$

The morphism f is said to be injective (respectively surjective) if the map of sets F is injective (resp. surjective). The morphism f is said to be an isomorphism if there exists an inverse morphism, that is a morphism of binary structures

$$g : (T, \perp) \to (S, *)$$

such that $g \circ f = Id_S$ and $f \circ g = Id_T$. Here Id_S (resp. Id_T) is the identity morphism of binary structures on $(S, *)$ (resp. $(T, \perp)$).

We break the problem into two parts. First we show that if f is an isomorphism, then it is both injective and surjective. Then we will show that if f is both injective and surjective, then f is an isomorphism.

[1] It is not necessary in your solutions to state all of the definitions first. I do this here for your convenience. It can also be a good place to start when you're trying to solve the problem – at least that way you know what the question is asking.

[2] Usually I will use the same notation for the map of sets (that is I will use f rather than F). However, in this problem, I think the solution is more clear if we make the pedantic choice to give the map of sets a different (but related) name.

2.1. **Part I: If f is an isomorphism, then it is both injective and surjective.**

> The basic idea of the proof is that an isomorphism of binary structures defines a bijection of sets, and we have seen that bijections are both injective and surjective.[3]

We now give a precise proof. Suppose f is an isomorphism. Using the same notation as above, let $g : (T, \perp) \to (S, *)$ be a morphism of binary structures such that $g \circ f = Id_S$ and $f \circ g = Id_T$. Let us use the notation

$$G : T \to S$$

for the map of sets included in the definition of g.

Recall that by the definition of the identity morphism of binary structures, the map of sets associated to Id_S (resp. Id_T) is the identity. Let us use the notation $ID_S : S \to S$ (resp. $ID_T : T \to T$) for the identity map of sets on S (resp. T).

Now, since $g \circ f = Id_S$ and $f \circ g = Id_T$, we have that

$$G \circ F = ID_S \quad \text{and} \quad F \circ G = ID_T.$$

Thus, F is a bijection of sets. We have proven in an earlier exercise that a bijection of sets is both injective and surjective. Thus the morphism f is both injective and surjective (since the map of sets F is).

2.2. **Part II: If f is both injective and surjective, then f is an isomorphism.**

> The basic idea of this proof is to use the fact that an injective and surjective map of sets is a bijection. One must then check that the inverse map of sets obtained in this way gives in fact a morphism of binary structures. One does this by using the fact that f is a morphism of binary structures.

We now give a precise proof. Suppose that f is both injective and surjective. This means that the map of sets $F : S \to T$ is both injective and surjective. We have proven in an earlier exercise that a map of sets that is both injective and surjective is a bijection; in other words, there exists a map of sets

$$G : T \to S$$

such that $G \circ F = ID_S$ and $F \circ G = ID_T$.

I claim that G induces a morphism of binary structures $g : (T, \perp) \to (S, *)$; in other words, I claim that for all $t_1, t_2 \in T$,

$$G(t_1 \perp t_2) = G(t_1) * G(t_2).$$

Let us check this now. Using the definition of a surjective map of sets, let $s_1 \in S$ (resp. $s_2 \in S$) be an element such that $F(s_1) = t_1$ (resp. $F(s_2) = t_2$). Note that $G(t_1) = G(F(s_1)) = (G \circ F)(s_1) = ID_S(s_1) = s_1$. Similarly, $G(t_2) = s_2$. Using this we have

$$\begin{aligned} G(t_1 \perp t_2) &= G(F(s_1) \perp F(s_2)) = G(F(s_1 * s_2)) = (G \circ F)(s_1 * s_2) \\ &= ID_S(s_1 * s_2) = s_1 * s_2 = G(t_1) * G(t_2). \end{aligned}$$

Note that the second equality holds from the fact that f is a morphism of binary structures. This establishes the claim, and hence that g is a morphism of binary structures. Since

[3] It can be nice to give a short outline of what you plan to do. This way the reader has the big picture in mind before they start to check the details.

$G \circ F = ID_S$ and $F \circ G = ID_T$, it follows that $g \circ f = Id_S$ and $f \circ g = Id_T$. This proves that f is an isomorphism.

2.3. **Conclusion.** In conclusion we have shown that if f is an isomorphism, then it is both injective and surjective, and conversely, that if f is both injective and surjective, then it is an isomorphism. This completes the proof.