1. Proposition D.1.

2. Proposition D.2. (Warning: The proof of this is not similar to those of Propositions 1.7 and 1.8 from Chapter 1: those proofs used the commutative axioms for \( \mathbb{Z} \), but here, you need to give a proof that’s valid even for nonabelian groups.)


For the next few problems, you will need the following definition. Let \( G \) and \( H \) be two groups. They are said to be **isomorphic** if there is a bijection \( f : G \rightarrow H \) such that for all \( g_1, g_2 \in G \), we have

\[
f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2).
\]

\((*)\)

In this case, \( f \) is said to be an **isomorphism**. Note that “\( \cdot \)” means **different** things on the two sides of this equation: on the left, it’s the operation in \( G \), but on the right, it’s the operation in \( H \).

**Examples:** Consider the groups \( S_2 = \{1 2, 1 2\} \) and \( H = \{1 2 3, 1 2 3\} \). (We discussed \( H \) in class on Wednesday, April 13; it’s an abelian subgroup of \( S_3 \).) The function \( f : S_2 \rightarrow H \) given by

\[
f(1 2) = 1 2 3, \quad f(1 2) = 1 2 3
\]

is an isomorphism. (Check that \((*)\) holds for all \( g_1, g_2 \in S_2 \).) So \( S_2 \) and \( H \) are isomorphic. That still doesn’t mean that every bijection between them is an isomorphism: the function \( q : S_2 \rightarrow H \) given by

\[
q(1 2) = 1 2 3, \quad q(1 2) = 1 2 3
\]

is a bijection but is not an isomorphism, because \( q((1 2) \cdot (1 2)) \neq q(1 2) \cdot q(1 2) \). (Check that.)

4. Prove that for any isomorphism \( f : G \rightarrow H \), we have \( f(1_G) = 1_H \). Here, \( 1_G \) denotes the identity element of \( G \), and \( 1_H \) denotes the identity element of \( H \). (Hint: You will need to use the “uniqueness” part of Proposition D.1.)

5. For any group \( G \), the identity function \( \text{id}_G : G \rightarrow G \) is an isomorphism from \( G \) to itself. Find an example of an isomorphism \( f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \) other than the identity function.

6. Prove that \( S_3 \) is not isomorphic to \( \mathbb{Z}_6 \). (They both have the same number of elements—namely, six—so there certainly exist bijections from \( S_3 \) to \( \mathbb{Z}_6 \). You have to prove that no bijection satisfies the extra condition \((*)\).)

7. (Bonus) Cayley’s Theorem: Every finite group is isomorphic to a subgroup of a symmetric group.