5 Group homomorphisms (09/29)

Definition 5.1 (Magma homomorphisms)**.** Let M and N be two magmas. A function $f\colon M \to N$ is a **magma homomorphism** if $f(ab) = f(a)f(b)$ for all $a, b \in M$.

Remark 5.2. The magma homomorphisms are the functions between the underlying sets that *respect the algebraic structures* given by the binary operations on M and N.

Definition 5.3. If G and H are groups, a function $f\colon G \to H$ is a **group homomorphism** if it is a homomorphism of the underlying magmas, i.e., if $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Remark 5.4. In the same way, one can define semigroup, monoid, quasigroup, and loop homomorphisms.

Lemma 5.5. *If $f\colon G \to H$ is a group homomorphism, then $f(e_G) = e_H$ where e_G is the identity element of G and e_H is the identity element of H.*

Proof. Since H is a group, $f(e_G)$ posseses an inverse, say a so that $af(e_G) = e_H$. We have $f(e_G) = f(e_Ge_G) = f(e_G)f(e_G)$; multiplying both sides on the left by a we obtain $e_H = af(e_G) = af(e_G)f(e_G) = e_Hf(e_G) = f(e_G)$, as desired. □

Lemma 5.6. *If $f\colon G \to H$ is a group homomorphism, then $f(a)^{-1} = f(a^{-1})$ for all $a \in G$.*

Proof. By uniqueness of inverses in groups, it is enough to show that $f(a^{-1})$ is an inverse for $f(a)$. But, $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H$, by Lemma 5.5, and similarly $f(a)f(a^{-1}) = e_H$. □

Example 5.7. Consider the exponential function $\exp\colon \mathbf{R} \to \mathbf{R}$ given by $\exp(x) = e^x$. As $\exp(x + y) = \exp(x)\exp(y)$, the map exp is a commutative monoid homomorphism $(\mathbf{R}, +) \to (\mathbf{R}, \times)$. If we delete 0, the function exp can be viewed as a group homomorphism $\mathbf{R} \to \mathbf{R}^\times$, where $\mathbf{R}^\times = \mathbf{R} - \{0\}$ is the *group* of non-zero elements of $\mathbf{R}$ under multiplication.

Example 5.8. We can also consider the function $f\colon (\mathbf{R}, +) \to (\mathbf{R}, \times)$ given by $f(x) = 0$ for all x. This is also a commutative monoid homomorphism. However, we do not have $f(0) = 1$, so it does not preserve the identity element of $(\mathbf{R}, +)$. This shows that the hypothesis that G and H be groups in Lemma 5.5 is necessary.

Definition 5.9. We say that a group homomorphism $f\colon G \to H$ is injective (one-to-one), surjective (onto), or bijective if the underlying function of sets is injective, surjective, or bijective.

Lemma 5.10. *A group homomorphism $f\colon G \to H$ is injective if and only if $f(x) = e$ implies $x = e$.*

Proof. Suppose that $f(x) = f(y)$ for some $x, y \in G$. Then, $e = f(e) = f(x^{-1})f(x) = f(x^{-1})f(y) = f(x^{-1}y)$, so $x^{-1}y = e$, or $y = x$. □

Lemma 5.11. *Suppose that $f\colon G \to H$ is a bijective group homomorphism. Let $f^{-1}\colon H \to G$ be the inverse function. Then, f^{-1} is a group homomorphism (which is again bijective).*

Proof. Let $x, y \in H$. We have to prove that $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Write $x = f(a)$ and $y = f(b)$, for unique $a, b \in G$, using that f is a bijection. Then, $f(ab) = f(a)f(b) = xy$, so that $f^{-a}(xy) = ab = f^{-1}(x)f^{-1}(y)$. □

Definition 5.12. A bijective group homomorphism is called a **isomorphism**. Two groups G and H are called **isomorphic** if there exists a group isomorphism $f\colon G \to H$.

Example 5.13. Let $\mathbf{R}^\times_+$ be the group of positive real numbers under multiplication. The exponential map $\exp\colon \mathbf{R} \to \mathbf{R}^\times_+$ is an isomorphism, so $\mathbf{R} \cong \mathbf{R}^\times_+$.

Remark 5.14. If G is a group, then the identity function id_G is a group isomorphism. If $f\colon G \to H$ and $h\colon H \to K$ are group isomorphisms, then so is $h \circ f\colon G \to K$. Using these facts and Lemma 5.11, it follows that the relation $G \cong H$ if G and H are isomorphic is an equivalence relation on the class of groups.

Example 5.15. Let G and H be groups with 1 element. Then, $G \cong H$. In particular, $S_0 = S_\emptyset$ and S_1 are isomorphic.

Example 5.16. There is an isomorphism $\mathbf{Z}/2 \to S_2$, so $\mathbf{Z}/2 \cong S_2$.

Example 5.17. If G is a group of order 2 (i.e., the underlying set has exactly 2 elements), then $G \cong \mathbf{Z}/2$.

Example 5.18. If G is a group of order 3, then $G \cong \mathbf{Z}/3$.

Definition 5.19 (Cyclic groups)**.** A group G is **cyclic** if $G \cong \mathbf{Z}$ or $G \cong \mathbf{Z}/N$ for some $N \geqslant 1$.

Example 5.20. Let $K = \mathbf{Z}/2 \times \mathbf{Z}/2$ be the product of two copies of $\mathbf{Z}/2$, with addition defined componentwise, so that $(a, b) + (c, d) = (a + c, b + d)$ where $a + c$ and $b + d$ are computed in $\mathbf{Z}/2$. This is a group with 4 elements, but K is not isomorphic to $\mathbf{Z}/4$. Indeed, $\mathbf{Z}/4$ has an two elements of order 4, but K has no element of order 4.

5.1 Exercises

Exercise 5.1. Prove that if $n \geqslant 3$, then S_n is not cyclic.

Exercise 5.2. Recall the group $(\mathbf{Z}/N)^\times$ from Exercise 3.4. Let $\phi(N)$ be the number of elements of $(\mathbf{Z}/N)^\times$. The function ϕ is called the **Euler totient function**.[1]

(a) Show that if $M, N \geqslant 1$ are relatively prime, then $\phi(MN) = \phi(M)\phi(N)$.

(b) Show that if $n \geqslant 1$, then for every prime number p we have $\phi(p^n) = p^{n-1}\phi(p)$.

(c) Show that $\phi(p) = p - 1$ if p is prime.

(d) What is $\phi(3072)$?

Exercise 5.3. Let $f\colon X \to Y$ be a bijection. Consider the permutation groups S_X and S_Y and the function $g\colon S_X \to S_Y$ defined by $g(h) = f \circ h \circ f^{-1}$ for $h \in S_X$. Prove that g is a group isomorphism.

[1] This is just a name. As far as I know, "totient" does not mean anything else.