Lectures in Group Theory

MOHAMMED ALABBOOD

University of Basrah-College of Science
Department of Mathematics

July 1, 2020

Some basic properties of homomorphisms

Let us prove some basic properties of homomorphisms.
Theorem: Let f be a homomorphism of a group G into a group G'. Then

1. $f(e) = e'$.
2. $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.
3. If $H \leq G$, then $f(H) = \{f(h) : h \in H\}$ is a subgroup of G'.
4. If H' is a subgroup of G', then $f^{-1}(H') = \{g \in G : f(g) \in H'\} \leq G$, and if $H' \trianglelefteq G'$, then $f^{-1}(H') \trianglelefteq G$.
5. If G is commutative, then $f(G)$ is commutative.
6. If $a \in G$ is such that $o(a) = n$, then $o(f(a))$ divides n.

Some basic properties of homomorphisms

Proof:

1. Since f is a homomorphism, $f(e)f(e) = f(ee) = f(e) = f(e)e'$. This implies that $f(e) = e'$ by the cancellation law.
2. Let $a \in G$. Then $f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$. Similarly, $f(a^{-1})f(a) = e'$. Since $f(a)$ has a unique inverse, $f(a^{-1}) = f(a)^{-1}$.
3. $f(e) = e'$ implies $e' = f(e) \in f(H)$ and so $f(H) \neq \emptyset$. Let $f(a), f(b) \in f(H)$, where $a, b \in H$. Since H is a subgroup, $ab \in H$. Thus, $f(a)f(b) = f(ab) \in f(H)$. Finally, $f(a)^{-1} = f(a^{-1}) \in f(H)$ Hence, $f(H)$ is a subgroup of G'
4. **Homework**.
5. Let $f(a), f(b) \in f(G)$. Then $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$. Hence, $f(G)$ is commutative.
6. Since $(f(a))^n = f(a^n) = f(e) = e'$, we have $o(f(a))$ divides n.

The kernel and image of homomorphisms

Let f be a homomorphism of a group G into a group G'. The **kernel** of f, written $\ker f$, is defined to be the set $\ker f = \{a \in G : f(a) = e'\}$. The image of f, written $\operatorname{im} f$, is defined to be the set $\operatorname{im} f = \{f(a) \in G' : a \in G\}$.

Example: Define $f : (\mathbb{Z}, +) \to (\mathbb{Z}_6, +)$ by $f(a) = r$, where r is the remainder when we divide a by 6. Note that f is a homomorphism: $f(a + b) = r = r_1 + r_2$, where r_1, r_2 are the remainders when a, b are divided by 6 respectively. It follows that $f(a + b) = r = r_1 + r_2 = f(a) + f(b)$. Now,

$$\begin{aligned} \ker f &= \{a \in \mathbb{Z} : f(a) = 0\} \\ &= \{a \in \mathbb{Z} : r = 0\}, \text{where } r \text{ is the remainder when we divide } a \text{ by } 6 \\ &= \{a = 6q : q \in \mathbb{Z}\} = 6\mathbb{Z}. \end{aligned}$$

Also, we have

$$\begin{aligned} \operatorname{im} f &= \{f(a) \in \mathbb{Z}_6 : a \in \mathbb{Z}\} \\ &= \{r \in \mathbb{Z}_6 : a \in \mathbb{Z}\}, \text{where } r \text{ is the remainder when we divide } a \text{ by } 6 \\ &= \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6. \end{aligned}$$