Proof on Some Statements

FIRDAUS Rafi Rizqy / 062101889

Special Mathematics Lecture: Groups and their representations (Fall 2022)

Exercise 1.1.3

1) *Observe that for any group G, the identity element e is unique.*

Proof: Suppose e, f are distinct identity elements of a group G. Then, from the definition of the identity element (**Definition 1.1.1**), one can show that

$$\begin{aligned} e &= fe \\ &= ef \\ &= f \end{aligned}$$

This gives contradiction with our assumption that $e \neq f$. Therefore, for any group G, the identity element is unique.

2) *Observe that* $e^{-1} = e$, $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$. *It also follows from the definition that for any element a, its inverse* a^{-1} *is unique.*

Proof: From the definition, as the identity element $e \in G$, one has $e^{-1} = e^{-1}e = ee^{-1} = e$. For the second and third statements, one needs to prove that the inverse of any element a is unique which we want to prove by using a contradiction. Suppose $\exists b, c$ as the inverse elements of G with $b \neq c$ such that $ab = ac = e$ for an element $a \in G$, then one has

$$\begin{aligned} b &= be \\ &= b(ac) \\ &= (ba)c \\ &= ec \\ &= c \end{aligned}$$

Therefore, this contradicts our assumption that b and c are distinct elements, and thus the inverse of all elements in G is unique. Thus for the second statement, by using the previous knowledge that the inverse element of any element $a \in G$ is unique, one can multiply the left-hand side with the inverse of a which can be shown as follows $a^{-1}(a^{-1})^{-1} = e = aa^{-1} = a^{-1}a \implies (a^{-1})^{-1} = a$. For the third statement, one can use the same trick such that one has $(ab)(ab)^{-1} = e = aa^{-1} = aea^{-1} = a(bb^{-1})a^{-1} = (ab)b^{-1}a^{-1} \implies (ab)^{-1} = b^{-1}a^{-1}$.

3) *The equality $ab = ac$ implies the equality $b = c$. Similarly, $ba = ca$ implies $b = c$.*
Proof: Let us multiply the inverse of a by the left-hand side of the first equality

$$a^{-1}(ab) = a^{-1}(ac)$$
$$(a^{-1}a)b = (a^{-1}a)c$$
$$\implies b = c$$

With the same technique, let us prove the second equality

$$(ba)a^{-1} = (ca)a^{-1}$$
$$b(aa^{-1}) = c(aa^{-1})$$
$$\implies b = c$$

Exercise 1.2.2

Prove that the conjugation defines an equivalence relation, namely the following three properties are satisfied:

1) $a \sim a$ (reflexivity)
Proof: Let e be the identity element of G. Then, one has

$$\begin{aligned} a &= ea \\ &= eae \\ &= eae^{-1} \\ \implies a &\sim a \end{aligned}$$

2) $a \sim b$ then $b \sim a$ (symmetry)
Proof: $a \sim b$ implies that $a = cbc^{-1}$ for some c, c^{-1} in G. Thus, one can write

$$c^{-1}a = (c^{-1}c)bc^{-1}$$
$$c^{-1}ac = b(c^{-1}c)$$
$$b = c^{-1}ac$$
$$\implies b \sim a$$

3) $a \sim b$ and $b \sim c$, then $a \sim c$ (transitivity)
Proof: Let $a = fbf^{-1}$ and $b = gcg^{-1}$ for some f, g in G such that one has

$$\begin{aligned} a &= fbf^{-1} \\ &= f(gcg^{-1})f^{-1} \\ &= (fg)c(g^{-1}f^{-1}) \\ &= (fg)c(fg)^{-1} \end{aligned}$$

Since $fg \in G$ from the definition of group, this implies that $a \sim c$.