Abstract Algebra - Assignment 3

Jaan Tollander de Balsch, 452056

February 3, 2019

This report uses definitions by (Gallian, 2017) chapters Groups, Finite Groups, and Subgroups.

Problem 3

Let G be a group and let H and K be subgroups of G. Show that the set $HK := \{h \cdot k \mid h \in H, k \in K\}$ is a subgroup of G if and only if $HK = KH$.

In order to prove that HK is a subgroup of G if only if $HK = KH$ it needs to satisfy the subgroup test. In this case, we will be using the **Two-Step Subgroup Test**. The subset HK is **nonempty** because subsets H and K are non-empty.

Closure under operation: For all $a, b \in HK$ implies $a \cdot b \in HK$.

1) Let $a = h_1 \cdot k_1$ and $b = h_2 \cdot k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$.
2) The definition of HK implies that $h_1 \cdot k_1 \in H$ and $h_2 \cdot k_2 \in K$.
3) A further implication is that $h_1, k_1 \in H$ and $h_2, k_2 \in K$.
4) Therefore all $h \in H$ must be in K and all $k \in K$ must be in H for HK to be a subgroup of G.

Closure under inverse: For all $a \in HK$ implies $a^{-1} \in HK$.

1) Let $a = h \cdot k$ where $h \in H$ and $k \in K$.
2) Then $(h \cdot k)^{-1} \in HK$.
3) Equivalently $k^{-1} \cdot h^{-1} \in HK$.
4) Definition of HK implies $k^{-1} \in H$ and $h^{-1} \in K$.
5) Therefore all inverses of $h \in H$ must be in K and all inverses of $k \in K$ must be in H for HK to be a subgroup of G.

For HK to be a subgroup of G, subgroups H and K must be equivalent, and therefore $HK = KH$.

Problem 4

Let $GL_2(\mathbb{R})$ denote the group of all invertible 2×2-matrices with real entries. Let

$$A := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } B := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

(a)

Show that A and B are indeed invertible, and determine their order.

The inverses of A and B are

$$A^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

and

$$B^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The order of A is infinite because there does not exist a positive integer n such that $A^n = \mathbf{I}$

$$A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

The sequence B^1, B^2, B^3, B^4

$$\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right)$$

The order of B is 4 because of $B^4 = \mathbf{I}$.

(b)

Compute the product $A \cdot B$ and determine its order. What is your conclusion?

The product $A \cdot B$

$$A \cdot B = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

The sequence $(A \cdot B)^1, (A \cdot B)^2 ..., (A \cdot B)^6$

$$\left(\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right)$$

The order of $A \cdot B$ is 6 because of $(A \cdot B)^6 = \mathbf{I}$.

As a conclusion, the order of an element a in group G is the size the set of distinct elements generated by the powers of a.

Problem 5

Let a, b, and c be elements in a group G.

(a)

Show that a and a^{-1} have the same order.

Let the order of the element a be the smallest positive integer n such that

$$\begin{aligned} a^n &= e \\ (a^n)^{-1} &= e \\ (a^{-1})^n &= e. \end{aligned}$$

The socks-shoes property $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ implies that $(a^n)^{-1} = (a^{-1})^n$.

If there was a positive integer $m < n$ such that $(a^{-1})^m = e$ this would imply that $a^m = e$ which is a contradiction. Therefore n is also the smallest positive integer such that $(a^{-1})^n = e$. This implies that the order of a^{-1} is also n. The same logic also works for sections (b) and (c).

(b)

Show that $b^{-1} \cdot a \cdot b$ and a have the same order.

Let the order of the element $b^{-1} \cdot a \cdot b$ be the smallest positive integer n such that

$$\begin{aligned} (b^{-1} \cdot a \cdot b)^n &= e \\ (b^{-1} \cdot a \cdot b) \cdot (b^{-1} \cdot a \cdot b) \cdot \ldots \cdot (b^{-1} \cdot a \cdot b) &= e \\ b^{-1} \cdot a \cdot (b \cdot b^{-1}) \cdot a \cdot (b \cdot b^{-1}) \cdot \ldots \cdot (b \cdot b^{-1}) \cdot a \cdot b &= e \\ b^{-1} \cdot a^n \cdot b &= e \\ a^n &= b \cdot e \cdot b^{-1} \\ a^n &= e. \end{aligned}$$

This implies that the order of element a is also n.

(c)

Using (b), show that $a \cdot b$ and $b \cdot a$ have the same order. Deduce from this, that $a \cdot b \cdot c$ and $b \cdot c \cdot a$ have the same order.

Let the order of the element $a \cdot b$ be the smallest positive integer n such that

$$\begin{aligned}
(a \cdot b)^n &= e \\
a \cdot (b \cdot a)^{n-1} \cdot b &= e \\
a \cdot (b \cdot a)^{n-1} &= e \cdot b^{-1} \\
a \cdot (b \cdot a)^{n-1} &= b^{-1} \cdot e \\
(b \cdot a) \cdot (b \cdot a)^{n-1} &= e \\
(b \cdot a)^n &= e
\end{aligned}$$

This implies that the order of element $b \cdot a$ is also n. Using this property, we can also prove that the order of element $a \cdot b \cdot c$ is the same as the order of element $b \cdot c \cdot a$

$$\begin{aligned}
(a \cdot b \cdot c)^n &= e \\
(a \cdot b')^n &= e, \quad b' = b \cdot c \\
(b' \cdot a)^n &= e \\
(b \cdot c \cdot a)^n &= e.
\end{aligned}$$

References

Gallian, J., 2017. *Contemporary Abstract Algebra*. 9th ed. Cengage Learning.