MA347 – HW5

Jonathan Lam

February 4, 2021

1. Let G be a group and $a, b \in G$. Prove that $(aba^{-1})^n = ab^na^{-1}$ for each $n \in \mathbb{N}$.

   Proof. Let $A(n)$ be the proposition that this equation is true when the exponent is n. $A(1)$ is clearly true, since $(aba^{-1})^1 = aba^{-1} = ab^1a^{-1}$.

   Assume that this is true for $A(n)$ for some $n \in \mathbb{N}$. Then $(aba^{-1})^{n+1} = (aba^{-1})^n(aba^{-1}) = (ab^na^{-1})(aba^{-1}) = ab^n(a^{-1}a)ba^{-1} = ab^neba = ab^nba = ab^{n+1}a$, where e is the unit element of G. Thus $A(n)$ is true $\Rightarrow A(n+1)$ is true. By the first form of induction, $A(n)$ is true $\forall n \in \mathbb{N}$. □

2. Let $\mathbb{K} = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. For each $a \in \mathbb{K}^n$ and $A \in \mathrm{GL}(n, \mathbb{K})$. Define $f_{A,a} : \mathbb{K}^n \to \mathbb{K}^n$ by $f_{A,a}(x) = Ax + a$.

   (a) Prove that $f_{A,a}$ is a bijective map.

   (b) Let $\mathrm{Aff}(n, \mathbb{K}) = \{f_{A,a} : A \in \mathrm{GL}(n, \mathbb{K}) \text{ and } a \in \mathbb{K}^n\}$. Prove that $\mathrm{Aff}(n, \mathbb{K})$ is a group under composition operation.

   Proof. (a) Prove bijective by proving both one-to-one and onto.

   Injectivity Let $x, y \in \mathbb{K}^n$, and $f_{A,a}(x) = f_{A,a}(y)$. Then:

$$\begin{aligned} f_{A,a}(x) = Ax + a \Rightarrow x &= A^{-1}(f_{A,a}(x) - a) \\ f_{A,a}(y) = Ax + a \Rightarrow y &= A^{-1}(f_{A,a}(y) - a) \\ &= A^{-1}(f_{A,a}(x) - a) \\ &= x \end{aligned}$$

   $f_{A,a}(x) = f_{A,a}(y) \Rightarrow x = y$, thus injective.

   Surjectivity Let $x \in \mathbb{K}^n$. Let $y = A^{-1}(z - a) \in \mathbb{K}^n$. Then

$$\begin{aligned} f_{A,a}(y) &= A(A^{-1}(z - a)) + a \\ &= (AA^{-1})(z - a) + a \\ &= I_n(z - a) + a \\ &= (z - a) + a = z + (-a + a) = z + 0 = z \end{aligned}$$

   Thus $\forall x \in \mathbb{K}^n$ there exists $y \in \mathbb{K}^n$ such that $f_{A,a}(y) = x$, thus surjective.

(b) Show that $(\mathrm{Aff}(n, \mathbb{K}), \circ)$ is a group by showing that it follows the group axioms:

Associativity Composition of mappings of a set onto itself is always associative. In particular, let $f_1, f_2, f_3 \in \mathrm{Aff}(n, \mathbb{K})$. Let $x \in \mathbb{K}^n$. Then:

$$\begin{aligned}(f_1 \circ (f_2 \circ f_3))(x) &= f_1((f_2 \circ f_3)(x)) \\ &= f_1(f_2(f_3(x))) \\ &= (f_1 \circ f_2)(f_3(x)) \\ &= ((f_1 \circ f_2) \circ f_3)(x)\end{aligned}$$

Thus $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$.

Identity element Let I_n denote the identity element of $\mathrm{GL}(n, \mathbb{K})$, and 0_n denote the zero element of $\mathbb{K}^n$. Let $e = f_{I_n, 0_n}$. Then for any $f_{A,a} \in \mathrm{Aff}(n, \mathbb{K})$ and any $x \in \mathbb{K}^n$:

$$\begin{aligned}(e \circ f_{A,a})(x) &= e(Ax + a) \\ &= I_n(Ax + a) + 0_n \\ &= Ax + a + 0_n \\ &= Ax + a \\ &= f_{A,a}(x)\end{aligned}$$

and

$$\begin{aligned}(f_{A,a} \circ e)(x) &= f_{A,a}(I_n x + 0_n) \\ &= f_{A,a}(x + 0_n) \\ &= f_{A,a}(x)\end{aligned}$$

thus $e \circ f_{A,a} = f_{A,a} = f_{A,a} \circ e$ for any $f_{A,a} \in \mathrm{Aff}(n, \mathbb{K})$.

Inverse element For any $f_1 = f_{A,a} \in \mathrm{Aff}(n, \mathbb{K})$, there exists $f_2 = f_{A^{-1}, -A^{-1}a} \in \mathrm{Aff}(n, \mathbb{K})$, and

$$\begin{aligned}(f_1 \circ f_2)(x) &= f_1(A^{-1}x - A^{-1}a) \\ &= A(A^{-1}x - A^{-1}a) + a \\ &= A(A^{-1}(x - a)) + a \\ &= (AA^{-1})(x - a) + a \\ &= I_n(x - a) + a \\ &= (x - a) + a \\ &= x + (-a + a) \\ &= x + 0_n = I_n x + 0_n = e(x)\end{aligned}$$

and

$$\begin{aligned}(f_2 \circ f_1)(x) &= f_2(Ax + a) \\ &= A^-1(Ax + a) - A^{-1}a \\ &= A^{-1}(Ax) + A^{-1}a - A^{-1}a \\ &= (A^{-1}A)x + A^{-1}(a - a) \\ &= I_n x + A^{-1}(0_n) = I_n x + 0_n = e(x)\end{aligned}$$

Thus $\forall f_1 \in \mathrm{Aff}(n, \mathbb{K})$, there exists $f_2 \in \mathrm{Aff}(n, \mathbb{K})$ such that $f_1 \circ f_2 = e = f_2 \circ f_1$.

$\square$