Abstract Algebra: Homework #1

Joel Savitz

Wednesday 27 May 2020

Note: for the scope of this document, let $\ni$ denote "such that".

1 Chapter 3: Excercise A1

Suppose $*$ is defined on $\mathbb{R}$ as $a*b = a+b+k$ for any $a, b \in \mathbb{R}$ for some $k \in \mathbb{R}$.

Theorem 1. *$\langle \mathbb{R}, * \rangle$ is a group.*

Proof. Let a, b, and c be some arbitrary real numbers. Because $a * b = a + b + k \in \mathbb{R}$, we have that the real numbers are closed under $*$. Then, observe that $a * (b * c) = a * (b + c + k) = a + (b + c + k) + k = (a + b + k) + c + k = (a + b + k) * c = (a * b) * c$, so $*$ is associative. We also have $a * -k = a + (-k) + k = -k + a + k = -k * a = a$, so $-k$ is the identity for the real numbers under $*$ Finally, consider the quantity $-(2k + a)$. Since we have $a * -(2k + a) = a + (-2k) + (-a) + k = -(2k + a) * a = -k$, that quantity is the inverse of any a. Since $*$ is closed under the real numbers and $*$ is associative and $-k$ is the identity of $*$ under the real numbers and any real number a has an inverse under $*$ of $-(2k - a)$, $\langle \mathbb{R}, * \rangle$ is a group. $\square$

2 Chapter 3: Exercise A3

Suppose $*$ is defined on $\mathbb{R}$ as $a * b = a + b + ab$ for any $a, b \in \mathbb{R}$.

Theorem 2. *$\langle \mathbb{R}, * \rangle$ is a group.*

Proof. Let a, b, and c be some arbitrary real numbers. Because $a*b = a+b+ ab \in \mathbb{R}$, we have that the real numbers are closed under $*$. Then, observe that

$a*(b*c) = a*(b+c+bc) = a+b+c+ab+ac+bc+abc = (a+b+ab)*c = (a*b)*c$, so $*$ is associative. We also have $a * 0 = a + (0) + 0a = 0 * a = a$, so 0 is the identity for the real numbers under $*$ Finally, consider the quantity $\frac{-a}{1+a}$. Since we have $a * \frac{-a}{1+a} = a + \frac{-a}{1+a} + \frac{-a^2}{1+a} = \frac{-a}{1+a} * a = \frac{a^2+a}{1+a} + \frac{-a}{1+a} + \frac{-a^2}{1+a} = 0$, that quantity is the inverse of any a. Since $*$ is closed under the real numbers and $*$ is associative and 0 is the identity of $*$ under the real numbers and any real number a has an inverse under $*$ of $\frac{-a}{1+a}$, $\langle \mathbb{R}, * \rangle$ is a group. □

3 Chapter 3: Exercise B1

Suppose $*$ is defined on $\mathbb{R} \times \mathbb{R}$ as $(a, b) * (c, d) = (ad + bc, bd)$ for any $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$.

Theorem 3. *$\langle \mathbb{R}, * \rangle$ is a group.*

Proof. Let $(a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R}$. Consider that $(a, b) * (c, d) = (ad + bc, bd) \in \mathbb{R} \times \mathbb{R}$ since $ad + bc \in \mathbb{R} \wedge bc \in \mathbb{R}$. Then, $\mathbb{R} \times \mathbb{R}$ is closed under $*$ Now observe the following equivalence: $\Big((a, b) * (c, d)\Big) * (e, f) = (ad + bc, bd) * (e, f) = (adf + bcf + bde, bdf) = (a, b) * (cf + de, df) = (a, b) * \Big((c, d) * (e, f)\Big)$ Since $(a, b) * (0, 1) = (1a + 0b, 1b) = (a, b) = (0b + 1a, 1b) = (0, 1) * (a, b)$, we have that $(0, 1)$ is the identity of the real numbers under $*$, Because we have $(a, b) * (\frac{-a}{b^2}, \frac{1}{b}) = (\frac{a}{b} + \frac{-a}{b}, b \cdot \frac{1}{b} = (0, 1) = (\frac{-a}{b} + \frac{a}{b}, \frac{1}{b}) = (\frac{-a}{b^2}, \frac{1}{b}) * (a, b)$, that pair $(\frac{-a}{b^2}, \frac{1}{b})$ is the inverse of any real a under 8. Then, since $*$ is a closed associative operation on the real numbers with an identity and an inverse for any element of the real numbers, we have that $\langle \mathbb{R}, * \rangle$ is a group.

□

4 Chapter 3: Exercise D

Suppose $*$ is defined as an operation on the set $A = \{I, V, H, D\}$ as follows in table 1:

Then, we have by table 1 that $*$ is a closed operation on A. Given that $*$ is associative, that I is an identity for $*$ by table 1, and that any $a \in A$ has the inverse $a \in a$ by table 1, we conclude that $\langle A, * \rangle$ is a group.

Furthermore, since we have that $*$ is commutative by table 1, $\langle A, * \rangle$ is an Abelian group.

$*$	I	V	H	D
I	I	V	H	D
V	V	I	D	H
H	H	D	I	V
D	D	H	V	I

Table 1: Operation table for $*$ on A

5 Chapter 3: Exercise E

Suppose some set A is defined as follows in equation 1:

$$A = \{I, M_1, M_2, M_3, M_4, M_5, M_6, M_7\} \tag{1}$$

The, suppose the binary operation $*$ is defined on A as follows in table 2:

$*$	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
I	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	M_1	I	M_3	M_2	M_5	M_4	M_7	M_6
M_2	M_2	M_3	I	M_1	M_6	M_7	M_4	M_5
M_3	M_3	M_2	M_1	I	M_7	M_6	M_5	M_4
M_4	M_4	M_6	M_5	M_7	I	M_1	M_2	M_3
M_5	M_5	M_4	M_7	M_6	M_1	M_3	I	M_2
M_6	M_6	M_7	M_4	M_5	M_2	I	M_3	M_1
M_7	M_7	M_6	M_5	M_4	M_3	M_1	M_2	I

Table 2: Operation table for $*$ on A

TODO: fix this table

6 A counterexample

Let $*$ be an operation defined on the set $G = \{x \in \mathbb{Z} \ni x \neq -1\}$ defines as $x * y = x + y + xy$.

Theorem 4. *$\langle G, * \rangle$ is not a group.*

Proof. Assume for the sake of contradictioion that G has an identity element and call it e. Then, we must have for any $a \in G$ that $a*e = a = a+e+ae \implies$

$e = -ae \implies a = -1$. However, $-1 \notin G$ and so we reach a contradiction, therefore our assumption must be wrong and there does not in fact exist an identity in G under $*$. Then, since a group must have an identity element and G has no identity element, G is not a group. $\square$

7 2×2 invertible matrices

Let $G = \{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{R}^{2\times2} \ni \exists A^{-1} \in \mathbb{R}^{2\times2} \ni AA^{-1} = A^{-1}A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\}$
Let $*$ be defined as standard matrix multiplication.

Theorem 5. *$\langle G, *\rangle$ is a group.*

Proof. Define the following three matrices $A, B, C \in \mathbb{R}^{2\times2}$ as follows:

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} C = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \tag{2}$$

Furthermore, suppose that matrices A and B are nonsingular, i.e. $A, B \in G$

The following equation defines a relationship between these matrices $C = A * B$ and the subsequent equation makes an observation about related determinants.

$$C = AB = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \cdot \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} = \begin{bmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{bmatrix} \tag{3}$$

$$det(C) = det(AB) = det(A) \cdot det(B) \neq 0 \tag{4}$$

Then, since C has real entries as demonstrated in equation 3 and since it is nonsingular as demonstrated by the nonzero determinant in equation 4, we conclude that $C \in G$ and that G is closed under $*$.

From this point on, A, B and C refer to nonasingular 2 by 2 matrices with arbitrary entries and no specific relationship to each other.

Consider the following arithmetic:

$$A * B = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \cdot \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} = \begin{bmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{bmatrix} \tag{5}$$

$$B * C = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \cdot \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{bmatrix} \tag{6}$$

$$A * (B * C) = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \cdot \begin{bmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{bmatrix} \tag{7}$$

$$= \begin{bmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_4c_3 & a_1b_1c_2 + a_1b_2c_4 + a_2b_3c_2 + a_2b_4c_4 \\ a_3b_1c_1 + a_3b_2c_3 + a_4b_3c_1 + a_4b_4c_3 & a_3b_1c_2 + a_3b_2c_4 + a_4b_3c_2 + a_4b_4c_4 \end{bmatrix} \tag{8}$$

$$(A * B) * C = \begin{bmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{bmatrix} \cdot \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \tag{9}$$

$$= \begin{bmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_4c_3 & a_1b_1c_2 + a_1b_2c_4 + a_2b_3c_2 + a_2b_4c_4 \\ a_3b_1c_1 + a_3b_2c_3 + a_4b_3c_1 + a_4b_4c_3 & a_3b_1c_2 + a_3b_2c_4 + a_4b_3c_2 + a_4b_4c_4 \end{bmatrix} \tag{10}$$

By equations 7 and 9, we have that G is associative under $*$.
Consider the following:

$$A * I = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = I * A \tag{11}$$

Then, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element of G.

Let us write A^{-1} to mean $\frac{1}{a_1a_4 - a_2a_3} \begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix}$ Consider one last set of equations:

$$A * A^{-1} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \cdot \frac{1}{a_1a_4 - a_2a_3} \begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix} = \begin{bmatrix} \frac{a_1a_4 - a_2a_3}{a_1a_4 - a_2a_3} & \frac{a_2a_4 - a_2a_4}{a_1a_4 - a_2a_3} \\ \frac{-a_1a_3 + a_1a_3}{a_1a_4 - a_2a_3} & \frac{-a_2a_3 + a_1a_4}{a_1a_4 - a_2a_3} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \tag{12}$$

$$A^{-1} * A = \frac{1}{a_1a_4 - a_2a_3} \begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \begin{bmatrix} \frac{a_1a_4 - a_2a_3}{a_1a_4 - a_2a_3} & \frac{a_2a_4 - a_2a_4}{a_1a_4 - a_2a_3} \\ \frac{-a_1a_3 + a_1a_3}{a_1a_4 - a_2a_3} & \frac{-a_2a_3 + a_1a_4}{a_1a_4 - a_2a_3} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \tag{13}$$

Then, any element $a \in G$ has an inverse $\frac{1}{a_1a_4 - a_2a_3}\begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix} \in G$.

Because G is closed under $*$, is associative, has an identity element, and has an inverse for each element,$\langle G, * \rangle$ is a group.

$\square$

Theorem 6. *$\langle G, * \rangle$ is not an Abelian group.*

Proof. Let $A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$. Notice that $AB = \begin{bmatrix} 0 & 1 \\ -2 & 1 \end{bmatrix}$ while $BA = \begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}$. Then, we have some $A, B \in G$ where $AB \neq BA$. We conclude that G is not commutative under $*$ and by definition G is not an Abelian group. $\square$

8 A subset of nonsingular 2 × 2 matrices

Let G be defined as follows:

$$G = \{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{R}^{2\times 2} \ni \exists A^{-1} \in \mathbb{R}^{2\times 2} \ni AA^{-1} = A^{-1}A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\wedge\, a + c = 1 \wedge b + d = 1\}$$

Let $*$ be defined on G as standard matrix multiplication.

Theorem 7. *$\langle G, * \rangle$ is a group.*

Proof. Let the definitions in equation 2 hold and suppose $C = AB$ as described by equation 3. We have the following equations by taking the sum of the colunms of C from equation 3:

$$a_1 + a_3 = a_2 + a_4 = b_1 + b_3 + b_2 + b_4 = 1 \quad (14)$$
$$a_1b_1 + a_2b_3 + a_3b_1 + a_4b_3 = b_1(a_1 + a_3) + b_3(a_2 + a_4) = b_1 + b_3 = 1 \quad (15)$$
$$a_1b_2 + a_2b_4 + a_3b_2 + a_4b_4 = b_2(a_1 + a_3) + b_4(a_2 + a_4) = b_2 + b_4 = 1 \quad (16)$$

Since the columns of C sum to 1, we have that $C \in G$ and in general that G is closed under $*$.

Now, suppose A, B and C are defined with generic real entries as described by equation 2.

By equations 7 and 9, we have that G is associative under $*$, since those equations hold for our current defintiion of G.

By the same reasoning demonstrated in equation 11, we have that $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity for G.

By the same reasoning demonstrated in equations 12 and 13, we have that $\frac{1}{a_1 a_4 - a_2 a_3} \begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix}$ is the inverse of any $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in G$.

Then, since G is closed under $*$, since G is associative under $*$, since G has an identity element and since every element of G has an inverse, we conclude that $\langle G, * \rangle$ is a group.

$\square$