Problem 2.3: Which of the following collections of 2×2 matrices with real entries form groups under matrix multiplication?

i) Those of the form $\begin{bmatrix} a & b \\ b & d \end{bmatrix}$ for which $ac \neq b^2$

Answer: The set of such matrices is not closed under matrix multiplication, so it does not form a group. To see that it is not closed under matrix multiplication, it is enough to consider the following example:

$$\begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} -2 & 5 \\ -3 & 7 \end{bmatrix}$$

where the matrix $\begin{bmatrix} -2 & 5 \\ -3 & 7 \end{bmatrix}$ is not of the form $\begin{bmatrix} a & b \\ b & d \end{bmatrix}$.

ii) Those of the form $\begin{bmatrix} a & b \\ c & a \end{bmatrix}$ such that $a^2 \neq bc$

Answer: Again, consider the two matrices $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 3 & 0 \\ 2 & 3 \end{bmatrix}$ which are of this form. Their product is $\begin{bmatrix} 7 & 6 \\ 2 & 3 \end{bmatrix}$, which is not in the correct form. So this set is not closed under matrix multiplication, and does not form a group.

iii) Those of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ where ac is not zero.

Answer: These do form a group. To show this, we need to check the following things.

(1) The set is closed under multiplication: Suppose $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ and $\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix}$ satisfy $ac, a'c' \neq 0$. Then

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} = \begin{bmatrix} a \cdot a' & a \cdot b' + b \cdot c' \\ 0 & c \cdot c' \end{bmatrix}$$

where $aa' \cdot cc' \neq 0$ because $ac, a'c' \neq 0$. Thus the product of two matrices in this set is again in the set, so it is closed under multiplication.

(2) The identity is in this set: This is true because the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is of the correct form.

(3) We have inverses: Suppose the matrix $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is in our set. Then consider the matrix $B = \begin{bmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$. Since $ac \neq 0$, the term $-\frac{b}{ac}$ makes sense, so B is well-defined. It is simple to check that $AB = BA = I$, where I is the identity matrix. Thus every matrix in our set has an inverse.

(4) Associativity: We have this because matrix multiplication is associative in general.

iv) The set of matrices with non-zero determinant and integer entries.

Answer: This set does not form a group because inverses may not be in the set. For example, consider the matrix $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$. This matrix is in our set. But its inverse is the matrix $\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$, which is not in our set.

Problem 2.6 Show that the collection of all rotations of the plane about a fixed point P forms a group under composition of functions. Is the same true of the set of all reflections in lines which pass through P? What happens if we take all the rotations and all the reflections?

Answer: Fix a point P in the plane. Let G_{ro} be the set of all rotations about P, let G_{re} be the set of all reflections about lines through P and let G be the set of all rotations and reflections together.

First, note that all of these sets satisfy the associativity property. This is because the composition of functions is always associative. Suppose we have three functions f, g and h. We need to see that for each point x in their domain, $f \circ (g \circ h)(x) = (f \circ g) \circ h(x)$. To show this takes just a bit of manipulation. Since $(g \circ h)(x) = g(h(x))$, we have $f \circ (g \circ h)(x) = f(g(h(x)))$, and likewise, $(f \circ g) \circ h(x) = (f \circ g)(h(x))$, which is again just $f(g(h(x)))$. Therefore, composition of functions is always associative, so composition of rotations and/ or reflections is also associative.

Now we show that G_{ro} is a group. Let $r_\theta \in G_{ro}$ be the clockwise rotation by angle θ about P. So if θ is negative, we mean a counter-clockwise rotation by $-\theta$. Then given two angles θ and ϕ, we clearly have $r_\theta \circ r_\phi = r_{\theta+\phi}$. Thus the composition of two rotations is again a rotation, so G_{ro} is closed under composition of functions. Now we have to check the 3 group properties.

(1) Associativity: Composition of functions is associative.
(2) Identity: Clearly the identity is r_0, the rotation by angle 0, since for any angle θ, $r_\theta \circ r_0 = r_\theta = r_0 \circ r_\theta$.
(3) Inverses: Fix an angle θ. Then the inverse of r_θ is $r_{-\theta}$ since $r_\theta \circ r_{-\theta} = r_0 = r_{-\theta} \circ r_\theta$.

Thus the set of rotations is a group under function composition.

For the next parts of the problem, we use the following fact about the composition of two reflections.

Property 1. *Let $R_a, R_b \in G_{re}$ be reflections about lines a and b through the point P. Suppose the angle that line a sweeps out as it moves in a clockwise direction to line b is θ. Then $R_b \circ R_a = r_{\theta/2}$, where $R_b \circ R_a$ means we do R_a first and then R_b.*

Proof. Choose some point Q in the plane, where $Q \neq P$. Then as in the diagram, measure the *signed* acute angle between the line segment $\overline{QP}$ and line a. We say this angle is positive if when you use $\overline{QP}$ to sweep out the angle you go in a clockwise direction. Otherwise, the angle is negative. Call this signed angle θ_1. In the diagram, the angle is positive. Then the signed acute angle between the line segment $\overline{R_a(Q), P}$ and a is also θ_1. Now let θ_2 be the signed acute angle between $\overline{R_a(Q), P}$ and the line b. Again, the signed acute angle between $\overline{R_b \circ R_a(Q), P}$ and the line b is also θ_2.

Note that the distance between Q and P is the same as the distance between $R_b \circ R_a(Q)$ and P. So if you rotate Q by an angle of $2\theta_1 + 2\theta_2$ about P, we get to $R_b \circ R_a(Q)$.

But $\theta_1 + \theta_2$ is just θ in the case when at least one of these two angles is positive, and $\theta_1 + \theta_2 = \theta - \pi$ when both of these angles are negative. So a rotation by $2\theta_1 + 2\theta_2$ is either a rotation by 2θ or a rotation by $2(\theta - \pi)$. But the latter is, in fact, the same as a rotation by θ since rotating by 2π is the same as not rotating at all. So we are done.

□

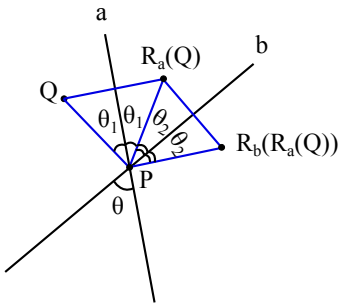

FIGURE 1. The point Q reflected first through a and then through b

By the above property, we see that the set of reflections is not closed under composition of functions, as two reflections give a rotation. So G_{re} is not a group.

On the other hand, we claim that G is a group.

Claim 1. *The set of all rotations and reflections forms a group.*

Proof. . It isn't hard to see by the same methods as above that if r_θ is a rotation and R_a is a reflection about a line a then

$$r_\theta \circ R_a = R_{r_{\frac{1}{2}\theta}(a)}$$

that is, reflecting about a and then rotation by angle θ is the same as reflecting about the line a rotated by angle $\frac{1}{2}\theta$. Likewise,

$$R_a \circ r_\theta = R_{r_{-\frac{1}{2}\theta}(a)}$$

So the set G of rotations and reflections is closed under composition of functions.

The identity is in G, because the identity is rotation by angle 0. Inverses are in G because each reflection is its own inverse, and the inverse of a rotation by angle θ is a rotation by angle $-\theta$. The set is associative because, again, composition of functions is associative. Therefore, G is a group. □

Problem 2.8 If x and y are elements of a group, prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Proof. The element $(xy)^{-1}$ is the element s.t. $(xy)^{-1}(xy) = 1 = (xy)(xy)^{-1}$. We show that the element $y^{-1}x^{-1}$ satisfies this property.

$$\begin{aligned}(y^{-1}x^{-1})(xy) &= y^{-1}(x^{-1}(xy)) \text{ by associativity}\\ &= y^{-1}((x^{-1}x)y) \text{ by associativity}\\ &= y^{-1}y \text{ by prop. of inverses}\\ &= 1 \text{ by prop. of inverses}\end{aligned}$$

so the first part of that equation is satisfied. Now for the second part.

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= ((xy)y^{-1})x^{-1} \text{ by associativity}\\ &= (x(yy^{-1}))x^{-1} \text{ by associativity}\\ &= x^{-1}x \text{ by prop. of inverses}\\ &= 1 \text{ by prop. of inverses}\end{aligned}$$

So we have shown that $(xy)^{-1} = y^{-1}x^{-1}$. □

Problem 3.2 Write $\mathbb{Q}(\sqrt{2})$ for the set described in Exercise 3.1 (iii). Given a non-zero element $a+b\sqrt{2}$ express $1/(a+b\sqrt{2})$ in the form $c+d\sqrt{2}$ where $c, d \in \mathbb{Q}$. Prove that multiplication makes $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ into a group.

Proof. The set $\mathbb{Q}(\sqrt{2})$ consists of all real numbers of the form $a+b\sqrt{2}$ where a and b are in $\mathbb{Q}$. The number $1/(a+b\sqrt{2})$ is the unique real number with the property that $(a+b\sqrt{2}) \cdot 1/(a+b\sqrt{2}) = 1$. Let $c = \frac{a}{a^2-2b^2}$ and let $d = -\frac{b}{a^2-2b^2}$. Then we claim that $1/(a+b\sqrt{2}) = c+d\sqrt{2}$. To see this, we calculate:

$$(a+b\sqrt{2}) \cdot c + d\sqrt{2} = ac + 2bd + (ad+bc)\sqrt{2}$$

Then

$$\begin{aligned} ac+2bd &= \frac{a^2}{a^2-2b^2} - \frac{2b^2}{a^2-2b^2} \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} ad+bc &= -\frac{ab}{a^2-2b^2} + \frac{ba}{a^2-2b^2} \\ &= 0 \end{aligned}$$

.

Thus, for the above choices of c and d, $(a+b\sqrt{2}) \cdot c + d\sqrt{2} = 1$, as promised.

Now we show that the set $G = \mathbb{Q}(\sqrt{2}) \setminus \{0\}$ is a group. The formula $(a+b\sqrt{2}) \cdot c+d\sqrt{2} = ac+2bd+(ad+bc)\sqrt{2}$ shows that this set is closed under multiplication. Since G is a subset of real numbers, it is associative. The identity is in G since $1 = 1+0\sqrt{2}$. Finally, the above calculation means that every non-zero element of $\mathbb{Q}(\sqrt{2})$ has a multiplicative inverse also in $\mathbb{Q}(\sqrt{2})$. Therefore, $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ is a group. □

Problem 3.3 Let n be a positive integer and let G consist of all those complex numbers z which satisfy $z^n = 1$. Show that G forms a group under multiplication of complex numbers.

Proof. First we show that G is closed under multiplication. Let $z, z' \in G$. We need to show that $(zz')^n = 1$. We have that

$$(zz')^n = \underbrace{zz' \cdot \cdots \cdot zz'}_{n \text{ times}}$$

But multiplication in $\mathbb{C}$ is commutative, so in fact, $(zz')^n = z^n z'^n$. Since $z, z' \in G$, this just means that $(zz') = 1$. Thus G is closed under multiplication.

Since $\mathbb{C}$ is a group, and G is a subset of $\mathbb{C}$, we know that G is associative. The identity is in G because $1^n = 1$. So the last thing we need to show is that G has inverses. Let $z \in G$. Then z^{-1} is some complex number (since all complex numbers have inverses which are complex numbers). We need to show that $(z^{-1})^n = 1$. But we know that $z^n = 1$. So multiply both sides of this equation by $(z^{-1})^n$. This gives us that $(z^{-1})^n z^n = (z^{-1})^n$. But $(z^{-1})^n z^n = 1$ by the fact that multiplication in $\mathbb{C}$ is commutative, so this means that $1 = (z^{-1})^n$, as required. Thus G is a group under multiplication. □

Problem 3.5 Let n be a positive integer. Prove that $(x \cdot_n y) \cdot_n z = x \cdot_n (y \cdot_n z)$.

Proof. By definition, $(x \cdot_n y) = xy - kn$ where $k \in \mathbb{Z}$ is the number s.t. $xy - kn \in [0, n-1]$. Thus,

$$\begin{aligned}(x \cdot_n y) \cdot_n z &= (xy - kn) \cdot_n z \\ &= (xy - kn)z - k'n \\ &= xyz - k''n\end{aligned}$$

where k' is the number s.t. $(xy - kn)z - k'n \in [0, n-1]$ and so $k'' = kz + k'$ is the number s.t. $xyz - k''n \in [0, n-1]$. With similar steps we get

$$\begin{aligned}x \cdot_n (y \cdot_n z) &= x \cdot_n (yz - ln) \\ &= x(yz - ln) - l'n \\ &= xyz - l''n\end{aligned}$$

where again l'' is the number s.t. $xyz - l''n \in [0, n-1]$. We want to show that $xyz - k''n$ and $xyz - l''n$ are the same number. Note that $xyz - k''n - (xyz - l''n) = (l'' - k'')n$. So the difference between these two numbers is an integer multiple of n. On the other hand, both $xyz - k''n$ and $xyz - l''n$ are between 0 and $n-1$. So $-(n-1) \leq xyz - k''n - (xyz - l''n) \leq n-1$. The only multiples of n inside these bounds is 0. Thus $l'' - k'' = 0$ and so $xyz - k''n = xyz - l''n$. Therefore, $(x \cdot_n y) \cdot_n z = x \cdot_n (y \cdot_n z)$. □

Problem 3.7 Which of the following sets form a group under multiplication modulo 14?

Answer: Note that $5 \cdot 5 = 11 \bmod 14$. The sets $\{1, 3, 5\}$ and $\{1, 3, 5, 7\}$ contain 5 and not 11, so they cannot form groups. The set $\{1, 7, 13\}$ cannot form a group mod 14 since 7 and 14 share a common factor, so 7 cannot have an inverse mod 14. In fact, suppose $7 \cdot_{14} x = 1$. Then $2 \cdot_{14} 7 \cdot_{14} n = 2$. But $2 \cdot_{14} 7 = 0$, so $0 = 2 \bmod 14$, which is impossible.

Finally, $9 \cdot_{14} 13 = 5$, so the set $\{1, 9, 11, 13\}$ does not form a group. So none of these sets form groups mod 14.

Problem 3.8 Show that if a subset of $\{1, 2, \ldots, 21\}$ contains an even number, or contains the number 11, then it cannot form a group under multiplication.

Proof. Suppose n is an even integer between 1 and 21, inclusive. Then we can write $n = 2m$ for some other integer m. We claim that n cannot have an inverse mod 22.

Suppose not. Then $n = 2m$ has an inverse with the property that $2m \cdot_{22} n^{-1} = 1$. Thus, $11 \cdot_{22} 2m \cdot_{22} n^{-1} = 11$. By associativity, I can multiply 11 and 2 first. Note that $11 \cdot_{22} 2 = 0$. Thus I get the statement that $0 \cdot_{22} n^{-1} = 11$, i.e. $0 = 11$. But this is not true mod 22. Therefore, n has no inverse.

Similarly, suppose $n = 11$. We claim that 11 cannot have an inverse mod 22.

Suppose not. Then $n = 11$ has an inverse with the property that $11 \cdot_{22} n^{-1} = 1$. Thus, $2 \cdot_{22} 11 \cdot_{22} n^{-1} = 2$. By associativity, I can multiply 11 and 2 first. Note that $11 \cdot_{22} 2 = 0$. Thus I get the statement that $0 \cdot_{22} n^{-1} = 2$, i.e. $0 = 2$. But this is not true mod 22. Therefore, 11 has no inverse.

So if we were given a subset of $\{1, 2, \ldots, 21\}$ containing the number 11 or any even number, then that subset couldn't possibly have inverses for all of its elements. Therefore it would not form a group. □

Problem 4.7 Let G be the collection of all rational numbers x which satisfy $0 \leq x < 1$. Show that the operation

$$x +_G y = \begin{cases} x + y & \text{if } 0 \leq x + y < 1 \\ x + y - 1 & \text{if } 1 \leq x + y < 2 \end{cases}$$

makes G into an infinite abelian group all of whose elements have finite order.

Proof. We will first show that G is a group. Again, we do this in four steps.

(1) G needs to be closed under the group operation. Let x, y be in G. Then $0 \leq x, y < 1$ so $0 \leq x + y < 2$. Thus $0 \leq x +_G y < 1$, so this is ok. Furthermore, both $x + y$ and $x + y - 1$ are rational numbers. So $x +_G y$ is a rational number between 0 and 1, as required.

(2) Identity. The identity is 0, which is in the group. To see that 0 is the identity, note that if $0 \leq x < 1$, then $0 \leq x + 0 < 1$, so $x +_G 0 = x$.

(3) Inverses. If $0 \leq x < 1$ then $0 \leq 1 - x < 1$. Note that $x + (1 - x) = 1$, so $x +_G (1 - x) = 0$. So for any $x \in G$, $1 - x$ is the inverse of x. Therefore the inverse of x is in G.

(4) Associativity. Let x, y and z be in G. Each time we add two numbers in G we subtract 1 enough times to make the result at least 0, and strictly less than 1. Since $0 \leq x + y + z < 3$, we see that

$$x +_G (y +_G z) = \begin{cases} x + (y +_G z) & \text{if } 0 \leq x + (y +_G z) < 1 \\ x + (y +_G z) - 1 & \text{if } 1 \leq x + (y +_G z) < 2 \end{cases}$$
$$= \begin{cases} x + y +_G z & \text{if } 0 \leq x + y + z < 1 \\ x + y + z - 1 & \text{if } 1 \leq x + y + z < 2 \\ x + y + z - 2 & \text{if } 2 \leq x + y + z < 3 \end{cases}$$

since $y +_G z$ is either $y + z$ or $y + z - 1$.

Similarly, we get that

$$(x +_G y) +_G z = \begin{cases} x + y +_G z & \text{if } 0 \leq x + y + z < 1 \\ x + y + z - 1 & \text{if } 1 \leq x + y + z < 2 \\ x + y + z - 2 & \text{if } 2 \leq x + y + z < 3 \end{cases}$$

Thus the group operation is associative.

Therefore, G is a group under this group operation.

There are infinitely many rational numbers between 0 and 1, so G is infinite. G is abelian because addition of rational numbers is abelian.

Finally, we need to show that elements of G have finite order. Let $\frac{a}{b}$ be an element of G. Then define

$$n \cdot_G \frac{a}{b} = \underbrace{\frac{a}{b} +_G \cdots +_G \frac{a}{b}}_{\text{n times}}$$

Since every time we add on another $\frac{a}{b}$ we subtract either 0 or 1, we have that $n \cdot_G \frac{a}{b} = \frac{na}{b} - m$ where m is an integer s.t. $0 \leq m \leq n$ and $0 \leq \frac{na}{b} - m < 1$. Thus for $n = b$, $b \cdot_G \frac{a}{b} = a - m$ where m is the integer s.t. $0 \leq a - m < 1$. But a is also an integer. So we must have $a = m$, and so $b \cdot_G \frac{a}{b} = 0$. But that means exactly that $\frac{a}{b}$ has order at most b, since adding $\frac{a}{b}$ to itself b times got us back to the identity. So every element of G has finite order. $\square$