MATH 335 Homework 4

Chris Camano: ccamano@sfsu.edu

September 22, 2022

1. Deterimine which one of the following sets is a group under addition:

   Proof of closure under addition:

   let our two elements be from the set G as follows:

$$a = \frac{a_m}{a_n} \quad b = \frac{b_m}{b_n}$$

$$\frac{a_m}{a_n} + \frac{b_m}{b_n} = \frac{a_m b_n + a_n b_m}{b_m b_n}$$

   Let $b_m = 2k+1, k \in Z \quad b_n = 2l+1, l \in \mathbb{Z}$

$$\frac{a_m b_n + a_n b_m}{b_m b_n} = \frac{a_m b_n + a_n b_m}{(2k+1)(2l+1)}$$

$$\frac{a_m b_n + a_n b_m}{b_m b_n} = \frac{a_m b_n + a_n b_m}{4kl+2k+2l+1}$$

   Thus since the denominator is still an odd number we have shown closure for the operation.

   the set of rational numbers in lowest terms whose denominators are odd

   a) *Proof.* Let G be the following set:

$$G = \left\{ \frac{m}{n}, n = 2k+1, n \neq 0, k, m \in \mathbb{Z} \right\}$$

   (a) Proof of associativity over operator let a,b,c∈G where:

$$a = \frac{a_m}{a_n} \quad b = \frac{b_m}{b_n} \quad c = \frac{c_m}{c_n}$$

$$\left(\frac{a_m}{a_n}+\frac{b_m}{b_n}\right)+\frac{c_m}{c_n}=\frac{a_m}{a_n}+\left(\frac{b_m}{b_n}+\frac{c_m}{c_n}\right)$$

$$\frac{a_mb_n+b_ma_n}{a_nb_n}+\frac{c_m}{c_n}=\frac{a_m}{a_n}+\left(\frac{b_mc_n+c_mb_n}{b_nc_n}\right)$$

$$\frac{c_n(a_mb_n+b_ma_n)+c_ma_nb_n}{a_nb_nc_n}=\frac{a_n(b_mc_n+c_mb_n)+a_mb_nc_n}{a_nb_nc_n}$$

$$\frac{c_na_mb_n+c_nb_ma_n+c_ma_nb_n}{a_nb_nc_n}=\frac{c_na_mb_n+c_nb_ma_n+c_ma_nb_n}{a_nb_nc_n}$$

The denominator $a_nb_nc_n$ is the product of three odd numbers which is also odd preserving the construction of G.

(b) Proof of existence of identity element
The Identity element for this set is the element: $\frac{0}{1}=0$

(c) Proof of existence of inverse of operator
For all g$\in G$ the additive inverse is the element $-g$

Thus we have proven that the set G and the operator of addition form a group. □

b) the set of rational numbers in lowest terms whose denominators are even

Proof. This set is not closed under the binary operator, consider the following example:

$$a=\frac{1}{6}\quad b=\frac{1}{6}$$

under addition this yields:

$$\frac{1}{6}+\frac{1}{6}=\frac{1}{3}\notin G$$

Thus since the binary operator fails under closure, this set and operation do **not** form a group □

c) the set of rational numbers of absolute value <1
Let G be the following set:

$$G=\left\{\frac{m}{n},n\neq 0,n,m\in\mathbb{Z},|\frac{m}{n}|<1\right\}$$

Proof. The binary operator of addition fails for this set when dealing with elements whose sum is greater than one. There are infinite examples of this, let us pick an apparent one:

$$a=\frac{1}{2}\quad b=\frac{1}{2}$$

$$a+b=\frac{1}{2}+\frac{1}{2}=1\notin G$$

Due to the fact that the binary operator fails for closure this operator and set G do **not** form a group □

d) the set of rational numbers of absolute value ≥ 1 together with 0.
Let G be the following set:

$$G = \left\{ \frac{m}{n}, n \neq 0, k, m \in \mathbb{Z}, |\frac{m}{n}| > 1 \right\} \cup \{0\}$$

Proof. Due to the construction of G taking the absolute value over each of its elements this opens weaknesses in the closure of the binary operator. We can easily pick negative values less than -1 and show that under addition with a positive element that we can arrive at a value less than 1 when the difference between our selection of a and b is satisfactory:

$$a = \frac{-5}{3} \quad b = \frac{3}{2}$$

$$a + b = \frac{-5}{3} + \frac{3}{2} = \frac{-1}{6} \notin G$$

Thus, again, since we fail under closure of the binary operator the set G does **not** form a group under the operator of addition ☐

2. Let $G = \{x \in \mathbb{R} : 0 \leq x < 1\}$ and for $x, y \in G$ let $x \cdot y$ be the fractional part of $x + y$ (i.e. $x \cdot y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\cdot$ is a binary operation on G and that G is a group.

Proof. Proof that $\cdot$ is a binary operator
For all x and y $\in G$ under out operator we are considering the sum of two numbers less than one and subtracting the greatest integer less than or equal to their sum leaving behind the remainder. Since the values of the elements of G are less than one then we have the following correspondence:

$$0 \leq x + y < 2$$

This implies that for all sums the maximum integer present can only be at most one since the sum is always less than two. Subtracting one from the sum when it is present will leave behind a fractional component that by definition would be element of G. Thus this implies closure under the operator. ☐

Proof. Proof that G is a group

(a) Proof of associativity over operator

$$\begin{aligned}
&(x \cdot y) \cdot z = (x \cdot y) \cdot z \\
&(x \cdot y) \cdot z = (x + y - [x + y]) \cdot z \\
&(x \cdot y) \cdot z = (x + y - [x + y]) + z - [(x + y - [x + y] + z] \\
&(x \cdot y) = x + y + z - [x + y] - [x + y + z] + [x + y] \\
&(x \cdot y) = x + y + z - [x + y + z] \\
&(x \cdot y) = x + y + z - [x + y + z] + [y + z] - [y + z] \\
&(x \cdot y) = x + y + z - [x + y + z - [y + z]] - [y + z] \\
&(x \cdot y) \cdot z = x \cdot (y \cdot z)
\end{aligned}$$

(b) Proof of existence of identity element
Consider the case of 0. $0 \in G$ and for all elements g in G:

$$g \cdot 0 = g + 0 - [g + 0] = g$$

(c) Proof of existence of inverse of operator
We need some element in G that takes us back to zero under our binary operator, let us solve for when this would happen. We would need to have a like term for the first sum of the two elements under the operator and a like term for the subtracted integer sum so that the difference will be 0 : For a given $g \in G$ consider the value (1-g). (1-g) is always in G since the elements of g are less than one. this gives:

$$\begin{aligned} &g + (1 - g) - [g + 1 - g] \\ &1 - [1] \\ &0 \end{aligned}$$

so we have shown that 1-g is the inverse of any g $\in G$ under our operator

Thus we have proven that our set G with our binary operator form a group. □

3. Let $G = \{z \in \mathbb{C} : z^n = 1$ for some nonnegative integer $n\}\{0$. Prove that G is a group under multiplication (called the groups of *roots of unity* in $\mathbb{C}$).

Proof. (a) Proof of Closure under operator: let :

$$a = z_1^a = 1 \quad b = z_2^b = 1$$

Take $z_{1,2} = z_1 z_2$ and $n_{1,2} = ab$

$$z_{1,2}^{ab} = (z_1 z_2)^{ab} = z_1^{ab} z_2^{ab} = (z_1^a)^b (z_2^b)^a = 1^b 1^a = 1$$

(b) Proof of associativity over operator
All elements in G are also elements of $\mathbb{C}$ so in turn they should all be associative under multiplication: proof:

Let $x, y, z \in \mathbb{C}$

$$\begin{aligned} (xy)z &= ((a+ib)(c+id))(e+if) \\ (xy)z &= ((ac-bd)+i(ad+cb))(e+if) \\ (xy)z &= ((ac-bd)e-(ad+cb)f)+i)(ac-bd)f+(ad+cb)e) \\ (xy)z &= (a(ce-df)-b(cf+ed))+i(b(ce-df)+a(ed+cf) \\ (xy)z &= (a+ib)((cf-df)+i(cf+ed)) \\ (xy)z &= x(yz) \end{aligned}$$

(c) Proof of existence of identity element The identity element of this set under the operation of multiplication is the number 1 which is an element of $\mathbb{C}$ This is because:

$$\forall z \in \mathbb{C} \quad 1^n z^n = z^n$$

(d) Proof of existence of inverse of operator
The inverse of a given element in G would be the term:

$$\tilde{z} = \left(\frac{1}{z}\right)^n = \frac{1}{z^n}$$

$\tilde{z} \in$ by the fact that:

$$z^n = 1$$
$$1 = \frac{1}{z^n}$$

Thus we have shown that this set with the binary operator of addition form a group. □

4. Let $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

a) Prove that G is a group under addition.

Proof. (a) Proof of Closure under operator let our two elements be:

$$a + b\sqrt{2} \quad x + y\sqrt{2}$$

$$a + b\sqrt{2} + x + y\sqrt{2} = (a + x) + (b + y)\sqrt{2}$$

This is an element of G and thus addition is a satisfactory binary operator

(b) Proof of associativity over operator
Let
$$a = a_1 + b_1\sqrt{2} \quad b = a_2 + b_2\sqrt{2}) \quad c = a_3 + b_3\sqrt{2}$$

$$(a + b) + c = a + (b + c)$$
$$(a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}) + a_3 + b_3\sqrt{2} = a_1 + (b_1\sqrt{2} + a_2 + b_2\sqrt{2} + a_3 + b_3\sqrt{2})$$
$$a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} + a_3 + b_3\sqrt{2} = a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} + a_3 + b_3\sqrt{2}$$

(c) Proof of existence of identity element Let $a = b = 0$ this the we have $0 + 0\sqrt{2} \in G$ which implies that $\forall g \in Gg + 0 = g$ Which means that 0 is our identity element.

(d) Proof of existence of inverse of operator
To identify the inverse of this group we need some value who when summed with a given g returns us to the identity. That value is the following: let$g = a + b\sqrt{2}$, the inverse would then be the following element
$$-a - b\sqrt{2}$$
as :
$$a + b\sqrt{2} + (-a - b\sqrt{2}) = 0$$

Thus the set G and the binary operation of addition form a group □

b) Prove that the nonzero elements of G are a group under multiplication ["Rationalize the denominators" to find the inverses].

Proof. (a) Proof of Closure under operator
let our two elements be the following:

$$a+b\sqrt{2} \quad x+y\sqrt{2}$$

$$\begin{aligned}&(a+b\sqrt{2})(x+y\sqrt{2})\\&ax+ay\sqrt{2}+bx\sqrt{2}+2by\\&(ax+2by)+(bx+ay)\sqrt{2}\end{aligned}$$

We have shown that this element is still in G since the product of the intermediate terms will always be an element of $\mathbb{Q}$ under closure of multiplication in $\mathbb{Q}$

(b) Proof of associativity over operator Let

$$a=a_1+b_1\sqrt{2} \quad b=a_2+b_2\sqrt{2}) \quad c=a_3+b_3\sqrt{2}$$

$$\begin{aligned}&(ab)c=a(bc)\\&(a_1+b_1\sqrt{2}(a_2+b_2\sqrt{2}))a_3+b_3\sqrt{2}=a_1+b_1\sqrt{2}(a_2+b_2\sqrt{2}(a_3+b_3\sqrt{2}))\\&(a_1a_2+a_1b_2\sqrt{2}+a_2b_1\sqrt{2}+2b_1b_2)a_3+b_3\sqrt{2}=a_1+b_1\sqrt{2}(a_2a_3+a_2b_3\sqrt{2}+a_3b_2\sqrt{2}+2b_2b_3)\\&a_1a_2a_3+a_1a_2b_3\sqrt{2}+a_1a_3b_2\sqrt{2}+2a_1b_1b_3+a_2a_3b_1\sqrt{2}+2a_2b_1b_3+2a_1b_1b_2a_3+2b_1b_2b_3\sqrt{2}=\\&a_1a_2a_3+a_1a_2b_3\sqrt{2}+a_1a_3b_2\sqrt{2}+2a_1b_1b_3+a_2a_3b_1\sqrt{2}+2a_2b_1b_3+2a_1b_1b_2a_3+2b_1b_2b_3\sqrt{2}\end{aligned}$$

(c) Proof of existence of identity element
Since we are dealing with multiplication typically the identity element is the concept of 1 . Here that concept manifests as the term:

$$1+0\sqrt{2}$$

And for all values in G multiplying any given value returns the original value thus this is our identity.

(d) Proof of existence of inverse of operator
To identitfy the multiplictive inverse we must solve the following equation:

$$\begin{aligned}&(a+b\sqrt{2})x=1\\&x=\frac{1}{a+b\sqrt{2}}\\&x=\frac{1}{a+b\sqrt{2}}\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}\end{aligned}$$

$\forall g\in G$ of the form $g=a+b\sqrt{2}$ we have the following:

$$a+b\sqrt{2}\left(\frac{a-b\sqrt{2}}{a^2-2b^2}\right)=\frac{a^2-2b^2}{a^2-2b^2}=1$$

Thus we have proven the existence of a multiplicitive inverse of the form:

$$\left(\frac{1}{a^2-2b^2}\right)a+\left(\frac{-1}{a^2-2b^2}\right)b\sqrt{2}$$

$\square$

Thus the set G and the binary operator of multiplication form a group.