Homework Assignment 1

Mark

September 11, 2024

Abstract

Note: This is my first time using LaTeX, feel free to point out areas of improvement. Furthermore, I used AI to help me with LaTeX syntax but did not use it for the math portions.

1 Problem 1

Let $n \in \mathbb{N}$, define the relation R on $S = \mathbb{Z}$ as follows: For $a, b \in \mathbb{Z}$, we have aRb if $a-b$ is divisible by n. Is R an equivalence relation on $\mathbb{Z}$? Justify your answer.
Solution: Relation R is an equivalence relation on $\mathbb{Z}$ iff the relation is reflexive, symmetric, and transitive. I will prove that R is an equivalence relation (assuming $0 \notin \mathbb{N}$)

Proof. 1. ***Reflexive:*** Assume $a \in \mathbb{Z}$, then aRa is $a - a|n = 0|n$. 0 is divisible by all numbers other than 0. R is reflexive. If $0 \in \mathbb{N}$, then this would not be an equivalence relation, because nothing is divisible by 0.

2. ***Symmetry:*** Assume aRb, then $a-b|n \implies a-b = n*k$ for some $k \in \mathbb{Z}$. We can multiply both sides by -1. $-1(a-b) = -1(n*k)$ which simplifies to $b - a = n*(-k)$, which is bRa. Therefore aRb implies bRa, specifically the resulting integer of bRa will be the negative of aRb

3. ***Transitivity:*** Suppose aRb and bRc. This means $a - b = k_1 n$ and $b-c = k_2 n$ for some $k, l \in \mathbb{Z}$.Adding these, we get $(a-b)+(b-c) = nk_1+nk_2 \implies a - c = (k_1 + k_2) * n$, where $k_1 + k_2 \in \mathbb{Z}$. Therefore, $aRb, bRc \implies aRc$

Because R is reflexive, symmetric, and transitive, R is an equivalence relation on $\mathbb{Z}$, assuming $0 \notin \mathbb{N}$. $\square$

2 Problem 2

Let $n \in \mathbb{N}$

2.1 Part (a)

Show that $(\mathbb{Z}\ n\mathbb{Z})$ is a monoid under the operation of multiplication. Assume $ab = a * b$, and that $(\mathbb{Z}\ n\mathbb{Z})$ is G
Solution: $(\mathbb{Z}\ n\mathbb{Z})$ is the set of equivalence classes $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. We must prove association and that an identity element exists.

Proof. 1. ***Associativity:*** We must prove that $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$. By definition $\overline{a} * \overline{b} = \overline{a * b}$ Thus, we can simplify both sides. The left-hand side simplifies to $\overline{a} * \overline{b * c} = \overline{a * b * c}$, while the right-hand side simplifies to $\overline{a * b} * \overline{c} = \overline{a * b * c}$, which are equal.

Therefore, $(\mathbb{Z}\ n\mathbb{Z})$ is associative.

2. ***Identity Element:*** We must prove that there exists some 1_G st $a * 1_G = a = 1_G * a \quad \forall a \in G$. Clearly, this element is $\overline{1}$, by definition $\overline{a} * \overline{1} = \overline{a * 1} = \overline{a}$

Therefore, $(\mathbb{Z}\ n\mathbb{Z})$ is a monoid. □

2.2 Part (b)

Show that $\overline{x}$ belongs to the unit group of $(\mathbb{Z}\ n\mathbb{Z})$ if and only if x and n are coprime
Solution:

Proof. 1. We will show that if x and n are coprime, then $\overline{x}$ belongs to $(\mathbb{Z}\ n\mathbb{Z})^X$. $\overline{x}$ exists in U_n iff there exists some inverse such that $\overline{x} * \overline{x^{-1}} \equiv \overline{1}$. Because Bézout's identity, we know that some $ax + bn = 1$, furthermore, because we are in the unit group, this fact can be used to say that $ax \equiv 1(modn)$. Therefore, in this set, x has an inverse a s.t. their product mod n is 1, and therefore they would (by definition) have to exist in the set □

2.3 Part (c)

List all the elements of the unit group $U(\mathbb{Z}\ 15\mathbb{Z})$. You may use results from part
Solution: Clearly 1. Because they need to be coprime, 3, 5, 6, 9, 10, and 12 are out. So, we are left with {1, 2, 4, 7, 8, 11, 13, 14} their respective inverses are {1, 8, 4, 13, 2, 11, 7, 14}

2.4 Part (d)

Find the orders of $\overline{2}, \overline{4}, \overline{7}$ in $U(\mathbb{Z}\ 15\mathbb{Z})$. Justify your answer **Solution:** The order of an element in a group is the lowest $n \in \mathbb{N}$ s.t. $g^n = 1_G$, in our case $\overline{g}^n \equiv 1(\bmod 15)$. I can just brute force this. 1. For $\overline{2}$, it is $2^4 = 16$, which mod 15 is 1. $n = 4$ 2. For $\overline{4}$, it is $4^2 = 16$. $n = 2$ 3. For $\overline{7}$, it is $7^4 = 2401$, which mod 15 is also 1 $n = 4$

3 Problem 3

Let G be the set of real numbers $(a, b) \in \mathbb{R}^2$ with $a \neq 0$ and define

$$(a, b) * (c, d) = (ac, ad + b) \quad 1_G = (1, 0)$$

Verify that this defines a group

Solution: G is a group iff it is associative, there is an identity element 1_G, and there is an inverse element $\forall (a, b) \in G$. Assume that $(a, b)(c, d) = (a, b) * (c, d)$

Proof. 1. ***Associativity:*** Manually check that $a(bc) = (ab)c$, or in our case $(a, b)((c, d)(e, f)) = ((a, b)(c, d))(e, f) \quad \forall (a, b), (c, d), (e, f) \in G$

$$(a, b)((c, d)(e, f)) = (a, b)(cd, cf + d) = (ace, a(cf + d) + b) = (ace, acf + ad + b)$$

$$((a, b)(c, d))(e, f) = (ac, ad + b)(e, f) = (ace, acf + ad + b)$$

These two equations are clearly equal, so G is associative.

2. ***Identity Element:*** We need to prove that the given identity element $1_G = (1, 0)$ holds all properties, specifically $(a, b)1_G = (a, b) = 1_G(a, b) \quad \forall a, b \in G$. Again, we can manually check that this is the case. Assume $(a, b) \in G$

$$(a, b)(1, 0) = (a, 0 + b) \quad (1, 0)(a, b) = (a, b + 0)$$

Clearly, this holds, therefore G has an identity element $1_G = (1, 0)$

3. ***Inverse Elements:*** We now must prove that $\forall (a, b) \in G$ there is some $(c, d) \text{st} (a, b)(c, d) = 1_G$. Suppose $(a, b) \in G$ and there is some $(c, d) \in G$. $(a, b)(c, d) = (ac, ad + b)$ for this to be the identity, we get two equations. $ac = 1 \quad \text{and} \quad ad + b = 0$, which solve to $c = \frac{1}{a} \quad \text{and} \quad d = -\frac{b}{a}$. Thus for every $(a, b) \quad a \neq 0$ has an inverse, specifically $(\frac{1}{a}, -\frac{b}{a}$

Because G is associative, has an identity element that follows all the rules, and has an inverse element for all sets, G is a group. ☐

4 Problem 4

For $\theta \in (0, 2\pi)$, define the rotation map R and the vertical mirror symmetric map S on the plane $\mathbb{R}^2$ as follows:

$$R(x, y) = (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta), \quad S(x, y) = (x, -y)$$

for $(x, y) \in \mathbb{R}^2$. Show that $RSR = S$.

Solution: We can simply manually check that this is the case. Take the set T. RSR on T would be to apply the map R, then S, then R again onto T, and show that that is the same as just applying S to T.

Proof. Let $(x, y) \in \mathbb{R}^2$. R on $\mathbb{R}^2 = (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta)$, next, RS on $\mathbb{R}^2 = (x \cos\theta - y \sin\theta, -x \sin\theta - y \cos\theta)$, next (grossly),

$$RSR \text{ on } \mathbb{R}^2 = ((x \cos\theta - y \sin\theta) \cos\theta - (-x \sin\theta - y \cos\theta) \sin\theta), (x \cos\theta - y \sin\theta) \sin\theta + (-x \sin\theta - y \cos\theta) \cos\theta$$

. This can be simplified into $x\cos^2\theta + x\sin^2\theta, -(y\sin^2\theta + y\cos^2\theta)$. Which, using trig identities, is just $(x, -y)$, which is the same result as applying S onto $\mathbb{R}^2$. Thus, applying $RSR : \mathbb{R}^2$ is the same as applying $S : \mathbb{R}^2$

□

5 Problem 5

Show that in a group $(G, *)$, the equations $a * x = b$ and $y * a = b$ are solvable for any $a, b \in G$.
Solution:

Proof. Suppose $a, b \in G$ and they have inverses $a^{-1}, b^{-1} \in G$. $a * x = b \to a^{-1} * a * x = a^{-1} * b$. By identity, $x = a^{-1} * b$. From this same logic $y * a = b \to y = b * a^{-1}$. This is solvable because $a, b, a^{-1}, b^{-1} \in G$, through our assumption and inverse rules. □

6 Problem 6

For an arbitrary group G, the center of G, denoted $C(G)$, is a subset of G consisting of all elements which commute with every element of G, that is,

$$C(G) := \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

For any group G, prove that $C(G)$ is a subgroup of G.
Solution: For $C(G)$ to be a subgroup of G, then $1_G \in C(G)$, $h, k \in C(G) \implies hk \in C(G)$, the inverse exists $\forall h \in C(G)$

Proof. 1. ***Identity Element:*** By definition, $1_G * x = x * 1_G \forall x \in G$, thus, the identity element must be in $C(G)$

2. ***Closed Under Products:*** Assume there exists some $h, k \in C(G)$. This implies that $hx = xh \quad \text{and} \quad kx = xk$. $khx = kxh$, by our equation $kx = xk$, we can pass hx as x, meaning that $k(xh) = (xh)k$ using our first equation, $(kh)x = x(kh)$ is proved directly, meaning that $\forall k, h \in C(G), kh \in C(G)$

3. ***Inverse exists:*** Assume there is $h \in C(G)$. By definition $hx = xh \forall x \in C(G)$ we can multiply both sides by the inverse of h $h^{-1}hxh^{-1} = h^{-1}xhh^{-1} \implies xh^{-1} = h^{-1}x$. So, $hx = xh$ implies $xh^{-1} = h^{-1}x$ □

7 Problem 7

Let G be a group, and assume that $X^2 = 1$ for all $x \in G$. Show that G is abelian.
Solution: Group G is abelian iff $ab = ba \quad a, b \in G$. We can prove this directly.

Proof. Assume some $x, y \in G$. We will prove that $xy = yx$ $x^2 = 1$, we can multiply both sides by the inverse of x, $x^{-1}xx = x^{-1}1 \rightarrow x = x^{-1} \forall x \in G$. Thus, $xy = x^{-1}y^{-1}$. The right-hand side can be simplified into $(yx)^{-1}$. Because the product of x and y is also in the group, we can use our first equation and get $(yx)^{-1} = (yx)$, which can be substituted as $xy = yx \forall x, y \in G$.

Therefore, G is abelian. □

8 Problem 8

Let G be a group. Show that

8.1 (Part (a))

For any $x, y \in G$, we have $o(x) = o(y^{-1}xy$ **Solution:** By definition, $o(x) =$ the smallest $n \in \mathbb{N}$ s.t. $x^n = 1_G$

Proof. Assume $x^n = 1_G$ and $(yxy^{-1})^m = 1_G$, and that $m \neq n$. We can expand the right side to be $1_G = yxy^{-1}yxy^{-1} \ldots yxy^{-1}$ (with m factors), and, using associativity and the identity property of inverses, we can simplify this to $1_G = yx^my^{-1}$. This leads to the conclusion that $1_G = x^m = x^n$.

Therefore, m must equal n. □

For any $a, b \in G$, we have $o(ab) = o(ba)$

8.2 (Part (b))

Solution: The solution here is pretty simple and just follows the definition and what we previously proved.

Proof. We know that $o(b) = o(a^{-1}ba)$. Now, we can simply take $b = ab$, subbing this in gives us $o(ab) = o(a^{-1}aba)$, which because of identity, is just $o(ab) = o(ba)$ □

9 Problem 9

Let G be a group and H be a non-empty subset of G. Show that H is a subgroup of G if and only if every $h \in H$ is invertible in G, and $h_1^{-1}h_2 \in H$ for all $h_1, h_2 \in H$

Solution: This can be proved essentially through definition. A subgroup must follow the following 3 properties. 1) $1_G \in H$, 2) $h, k \in H \implies hk \in H$, 3) $\forall h \in H \exists h^{-1}$

Proof. Assume $h_1, h_2, h_1^{-1} \in H$.
1. ***Identity Element:*** Because we are assuming that $\forall h \in H \exists h^{-1}$, by definition, their operation must be the identity element, and because those exact same elements exist in G, that identity element is also that of G

2. ***Closed Under Product:*** We can use some funny logic here. Because we are assuming that $h_1^{-1}h_2 \in H$ and that $h_1 \implies h_1^{-1}$, that means for every h in H, we know that the operation of it and every other element must exist, if we imagine h as the inverse of it's inverse.

3. ***Closed Under Product:*** This is assumed

$\square$