MAT301 Problem Set 1

Daniel Kats
997492468

January 29, 2014

1 Question 1

Let $G = \{(t, x) \mid |t, x \in \mathbb{R}, t \neq 0\}$. For (t_1, x_1) and (t_2, x_2) in G, define:

$$(t_1, x_1) * (t_2, x_2) = (t_1t_2, t_1x_2 + x_1/t_2)$$

1(a)

Prove that G is a group with respect to the operation *.

Proof. I will cover each group axiom in order:

Closure

Suppose $a = (t_1, x_1), b = (t_2, x_2) \in G$.

$$a * b = (t_1, x_1) * (t_2, x_2) = (t_1t_2, t_1x_2 + x_1/t_2)$$

Since $t_1 \neq 0$ and $t_2 \neq 0$ by definition, both the first and second elements of the resultant tuple are well defined and real. Moreover, $t_1t_2 \neq 0$. Thus $a * b \in G$.

Identity and Non-emptiness

Let $e = (1, 0)$. Clearly $e \in G$, so G is non-empty. Consider any element $a = (t, x) \in G$. Then $a * e = (t, t \cdot 0 + x/1) = (t, x) = a$. Thus G has an identity element, and it is e.

Inverse

I claim that if $a = (t, x)$, then $b = (\frac{1}{t}, -x)$ is an inverse for a. $a * b = (t \cdot \frac{1}{t}, -tx + tx) = (1, 0) = e$. Notice that as long as $t \neq 0$, the inverse exists, which is consistent with our definition of G.

Associativity

Let $a = (t_1, x_1), b = (t_2, x_2), c = (t_3, x_3) \in G$.

$$\begin{aligned}
(a * b) * c &= ((t_1t_2, t_1x_2 + x_1/t_2)) * (t_3, x_3) \\
&= (t_1t_2t_3, t_1t_2x_3 + \frac{t_1x_2 + x_1/t_2}{t_3}) \\
&= (t_1t_2t_3, t_1t_2x_3 + \frac{t_1x_2}{t_3} + \frac{x_1}{t_2t_3}) \qquad (1)
\end{aligned}$$

On the other hand:

$$\begin{aligned} a * (b * c) &= (t_1, t_2) * ((t_2 t_3, t_2 x_3 + x_2/t_3)) \\ &= (t_1 t_2 t_3, t_1 \cdot (t_2 x_3 + x_2/t_3) + \frac{x_1}{t_2 t_3}) \\ &= (t_1 t_2 t_3, t_1 t_2 x_3 + \frac{t_1 x_2}{t_3} + \frac{x_1}{t_2 t_3}) \end{aligned} \tag{2}$$

And notice that (1) and (2) are the same.

$\square$

1(b)

Find all elements belonging to the centre $Z(G)$ of G.

The elements in the center are all those elements $z = (a, b), a \neq 0$ which satisfy the equation:

$$tx = a^2 tx + ab - t^2 ab \tag{3}$$

For all tx and $t \neq 0$. Note that if $a \neq \pm 1, a \neq 0$, then our equation for z depends on x, which cannot be the case. So $a = \pm 1$. Then we have the equation $ab = t^2 ab$, which must be true for all non-zero values of t. This can only be accomplished by setting b to 0.

Thus the center is $Z(G) = \{(1, 0), (-1, 0)\}$.

2 Question 2

Let $G = D_6$ (the dihedral group of order 12). Let r be a fixed rotation in G such that $|r| = 6$ and let s be a fixed reflection in G.

2(a)

Let H be the smallest subgroup of G that contains rs and sr^3 . List all of the elements in H.

The elements of H are: $\{e = r^0, r^2, r^4, rs, sr, sr^3\}$. Notice that we have the following identities:

$$sr^3 = r^3 s, (rs)^2 = e, (sr^3)^2 = e, r^2 r^4 = e, (r^5 sr^3 s), (sr)^2 = e$$

We can see that H has closure, the identity element, and inverses. Also H is non-empty. Each of these elements is essential for closure or identity properties, so no smaller H can be found.

2(b)

Find an Abelian subgroup H' of D_6 that contains exactly 2 reflections.

Let r be a rotation of order 2. Let s_1 and s_2 be two reflections: s_1 is along the vertical axis, and s_2 is along the horizontal axis. Then let $H' = \{e, r, s_1, s_2\}$.

Then we have $rs_1 = s_2$, and $rs_2 = s_1$. This group is also Abelian, and each element is self-inverse.

I will give a quick outline of why this group is Abelian. First $s_1rs_1 = s_1s_1r^{-1} = er = r$. But $rs_1s_1 = re = r$. Now $s_1s_2 = s_1rs_1$ as before. We get similar results for s_2.

3 Question 3

3(a)

Let G be the group of functions from $\mathbb{Z}_{15}$ to $\mathbb{Z}_{15}$, under the operation $(f_1 \star f_2)(m) = (f_1(m)+f_2(m)) \pmod{15}, m \in \mathbb{Z}_{15}$. Let $H = \{f \in G \mid f(m) \text{ is even for all } m \in \mathbb{Z}_{15}\}$.

I do not think H is a subgroup, because I do not think inverses are well-defined, as $f \in H$ is by definition not onto. So by definition, there will be some elements $m \in \mathbb{Z}_15$ and $n \in \mathbb{Z}_15, m \neq n$ such that $f(m) = f(n)$. Thus $f^{-1}(f(n)))$ is not well-defined.

3(b)

Let $G = GL(2, \mathbb{R})$ and let $H = \left\{ A = \begin{bmatrix} a+b & -2b \\ b & a-b \end{bmatrix} \in G \mid a^2 + b^2 = 1 \right\}$.

First, H is non-empty, as setting $a = 0$ and $b = 1$ creates a valid matrix in H. Next, note that:

$$det(A) = (a^2 - b^2) + 2b^2 = a^2 + b^2 = 1$$

For the inverse, if $B \in H$, then we get:

$$B^{-1} = \frac{1}{det(B)} \begin{bmatrix} a-b & -(-2b) \\ -(b) & a+b \end{bmatrix} = \begin{bmatrix} a-b & 2b \\ -b & a+b \end{bmatrix}$$

Now suppose that $A \in H$ and $B \in H$. We know that multiplying the matrices together will result in some valid matrix in $GL(2, \mathbb{R})$, by properties of matrices. All we have to check is that $det(AB^{-1}) = det(A)det(B^{-1}) = \frac{det(A)}{det(B)} = 1$. Which is exactly the property we need. Thus H is a subgroup of G.

3(c)

Let G be the group of nonzero real numbers under multiplication and let $H = \{a + b\sqrt{2} \mid |a, b \in \mathbb{Z}, \text{at least one of } a \text{ and } b \text{ is nonzero}\}$.

Let $a = 2$ and $b = 2$. Then $c = a + b\sqrt{2} \in H$, and the value of c is $2 + 2\sqrt{2}$. Notice that the inverse of $2 + \sqrt{2}$ is $1 + \frac{-1}{2}\sqrt{2}$. There is no way to express the second number as an integer. Therefore $c^{-1} \notin H$. Thus H cannot be a subgroup of G.

4 Question 4

Let S be a subset of a group G. If $a \in G$, let $aSa^{-1} = \{asa^{-1} \mid s \in S\}$.

4(a)

Prove that S is a subgroup of G if and only if aSa^{-1} is a subgroup of G

Proof. $\Leftarrow$: Suppose that S is a subgroup of G. Also suppose $a \in G$. Since G is a group, $a^{-1} \in G$ also. Now take any element $s \in S$. Since S is a subgroup of G, $s \in G$. Therefore $as \in G$ by properties of groups. And also $asa^{-1} \in G$. This is true for any generic element $s \in S$. Therefore aSa^{-1} is a subgroup of G.

$\Rightarrow$: Suppose that aSa^{-1} is a subgroup of G, for some $a \in G$. Take arbitrary $b \in aSa^{-1}$. By definition, $b = asa^{-1}$ for some element s. I will show that $s \in G$ also. $ba \in G$ by properties of groups, and $ba = as$. Similarly $a^{-1} \in G$ as before, and $a^{-1}ba \in G$. So $s \in G$. □

4(b)

Suppose that $G = D_n$ ($n \geq 3$) and S is the set of all reflections in G. Prove that $aSa^{-1} = S$ for all $a \in G$.

Proof. There are two cases.

Case 1: a is a rotation Suppose that a is some rotation, and s is some reflection. Then $asa^{-1} = a^2s$, after left-multiplying both sides by a. Notice that a^2 is actually a rotation. But by another property of dihedral groups:

$$\text{any rotation} \cdot \text{any reflection} = \text{some reflection}$$

This property follows intuitively if we notice that there are only two types of elements in D_n: rotations and reflections. And if we color the "top" of the polygon white and the bottom black, then rotations maintain the color, while reflections flip the color. And since D_n has closure, any compound operation must be either a rotation or reflection. Thus for any rotation r, rs must be a reflection, since it changes the color of the polygon. In particular, a^2s is a reflection, so it is in S.

Case 2: a is a reflection Suppose that a is some reflection, and s is some reflection. Then $asa^{-1} = a^2s$, after left-multiplying both sides by a. However $a^2 = e$, by properties of reflections. Therefore $a^2s = s$, so trivially $asa^{-1} \in S$. □

5 Question 5

Let $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$. This is a group under the binary operation of multiplication modulo 16. That is, $mn = mn \pmod{16}$.

5(a)

Find all elements in the cyclic subgroup $\langle 3 \rangle$.

We have $\{11, 9, 3, 1\}$.

5(b)

Find an element $m \in U(16)$ such that $|m| = 4$ and $|\langle m \rangle \cap \langle 3 \rangle| = 2$. Is m unique?

Both 5 and 13 have this property. They are both in $U(16)$ (this is given). The order of 5 is 4, since $5^4 = 625 = 1 \pmod{16}$. Similarly $13^4 = 28561 = 1 \pmod{16}$. Finally:

$$\langle 5 \rangle = \langle 13 \rangle = \{1, 5, 9, 13\} \tag{4}$$

And the intersection of these sets with $\langle 3 \rangle$ is clearly just $\{1, 9\}$, which has order 2. In conclusion, m exists and is not unique.

5(c)

Determine whether $U(16)$ is a cyclic group.

I explicitly computed the order of each element, and none had order 8. Thus $U(16)$ is not cyclic.

6 Question 6

Let a and b be elements of a group G. Assume that both a and b have finite order.

6(a)

Prove that if $ab = ba$ and $gcd(|a|, |b|) = 1$, then $|ab| = |a||b|$.

Proof. It is clear that if $ab = ba$, then for any integer $n > 0$, $(ab)^n = a^n b^n$. By induction on n: if $n = 1$, then this is trivial. If $n > 1$, then:

$$(ab)^n = (ab)^{n-1}ab = a^{n-1}b^{n-1} = a^{n-1}b^{n-1}ba = a^{n-1}b^n a \tag{5}$$

But trivially b^n is also an element of G, so we can apply the rule again.

$$a^{n-1}b^n a = a^{n-1}ab^n = a^n b^n \tag{6}$$

Let $|a| = p$ and $|b| = q$. Let $n = pq$. This means $(ab)^n = (a^p)^q(b^q)^p = e^q e^p = e$. We know by theorem 4.1 Corollary 2 that $|ab|$ divides n. However, $n = pq$ and $gcd(p, q) = 1$ by the problem statement. Therefore $|ab|$ must be n. □

6(b)

Find an example of elements a and b in a particular group G such that $a \neq e$, $b \neq e$, $gcd(|a|, |b|) = 1$ and $|ab| = |a|$.

Consider D_3. Let r be a rotation such that $|r| = 3$. Let s be some reflection such that $|s| = 2$. $gcd(2, 3) = 1$. Then sr is a reflection (by properties of Dihedral groups), and thus has order 2, the same order as s. So let $a = s$ and $b = r$. We then get $|ab| = |sr| = 2$ and $|a| = |s| = 2$.