Math 212, Assignment 4

Solutions

All questions are equally weighted. They will be marked for correctness and clarity of explanation.

1. Let A be a cube and let G be the group of rotations that are symmetries of the cube. (Do not include any reflections.) For each point x given below, describe the set $G(x)$ and the subgroup G_x. Find $\#G(x)$ and $\#G_x$ in each case, where $\#X$ denotes the number of elements in the set X.

   Solution:

   (a) a corner of the cube.

   By rotating, the corner of the cube can be moved to any other corner of the cube: $G(x)$ = all corners of the cube, and $\#G(x) = 8$.
   The only motions which leave the corner x are rotations around a line which passes through x, through the centre of the cube and through the corner opposite to x. As there are three faces meeting at x, the rotation must permute these cyclicly; that is the rotation is through $0, 120$ or 240 degrees. These three rotations are G_x and $\#G_x = 3$.

   (b) the mid-point of an edge of the cube.

   By rotating the cube, this edge may be moved onto any other edge of the cube and the mid-point will be moved to the mid-point. So $G(x)$ consists of all mid-points of edges of the cube. There is one on each edge, so $\#G(x) = 12$.
   The only rotation (other than the identity) which fixes x must map the edge it lies on to itself by rotation by 180 degrees around a line that passes through x, through the centre of the cube and then through the mid-point of the edge opposite to x. So $\#G_x = 2$.

   (c) the centre of a face of the cube.

   By rotating the cube, the face may be moved onto any other face and the centre will be moved to the centre of the other face. As there are 6 faces, $G(x)$ will consist of 6 points.
   The rotations of the cube leaving x fixed must rotate around a line that passes through x, through the centre of the cube and then through the mid-point of the face opposite

to x. As these rotations must map the face to itself, they must be through $0, 90, 180$ or 270 degress. So $\#G_x = 4$.

2. Let L be the line

$$L = \left\{ \begin{bmatrix} x \\ 1 \end{bmatrix} \mid x \in \mathbb{R} \right\}$$

and let G be the $ax+b$-group which we view as a subgroup of S_L as in 3.8.13. Let

$$x = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

Find $G(x)$ and G_x.

Solution:

To find $G(x)$, we see what points on the line we can get by

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2a+b \\ 1 \end{bmatrix}$$

If $y = \begin{bmatrix} s \\ 1 \end{bmatrix}$ is any point on L, then we choose $b = s - 2$ and $a = 1$ and we get an element of the $ax+b$-group which moves x to y. Hence, $G(x) = L$.

For G_x, we need to find every matrix satisfying

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

This means we need

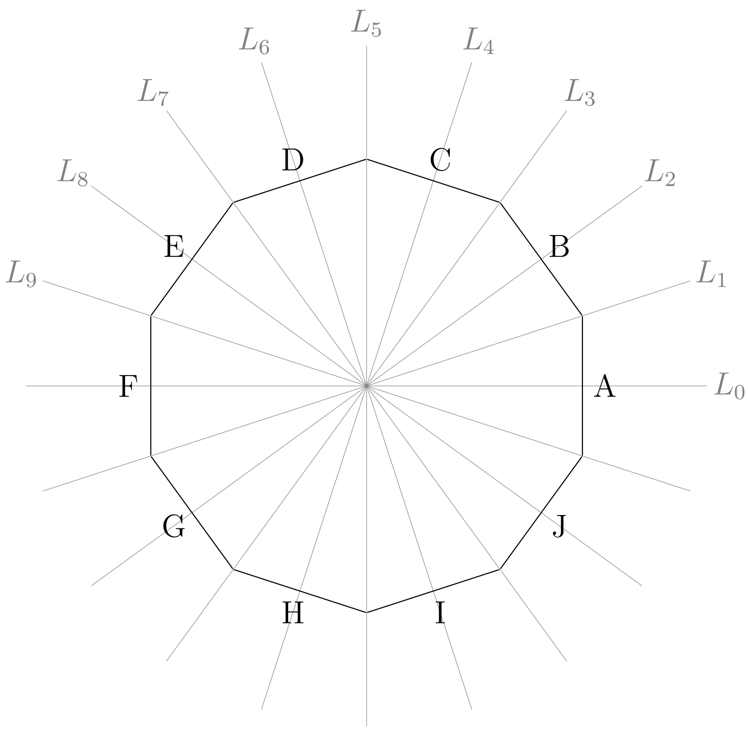
$$\begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2a+b \\ 1 \end{bmatrix}$$

or simply $2a + b = 2$. The a can be chosen to be any non-zero real number and then we let $b = 2 - 2a$.

$$G_x = \left\{ \begin{bmatrix} a & 2-2a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{R}, a \neq 0 \right\}.$$

3. Kevin is making beaded children's bracelets to sell at the community market. He has an unlimited supply of purple, blue, green and yellow beads. If each bracelet will have 10 beads, how many bracelet designs are possible?

Solution: We can think of the bracelet as a regular 10-gon, where each side represents a bead.



The group of symmetries of the bracelet is $D_{10} = \{e, r, r^2, \ldots, r^9, f_0, f_1, \ldots, f_9\}$, where r is a counterclockwise rotation by 36 degrees and for each $i = 0, 1, \ldots, 9$, f_i is a reflection over the line L_i.

For now, suppose the bracelet is fixed in place, and let A be the set of all colourings of the sides of the bracelet using purple, blue, green and yellow. We will use Burnside's Lemma to find the number of equivalence classes of A under the symmetries of D_{10}— that is, the number of inequivalent colourings of the bracelet when the bracelet can be rotated and flipped. To do this, we find the size of the fix set A^g for all $g \in D_{10}$.

For each $g \in D_{10}$, we count the number of ways to choose a colouring of the sides of the bracelet such that the colouring will be fixed by g.

- $g = e$: Since e does not move the bracelet, we get to choose a colour for each side independently. Therefore there are 4^{10} colourings of the bracelent that are fixed by e.
- $g = f_0$: We have 4 choices of colour for each of the sides A, B, C, D, E and G. Side G must be the same colour as E, H must be the same D, I must be the same as C and J must be the same as B. So in total we have 4^6 colourings that are fixed by f_0.

- $g = f_2, f_4, f_6, f_8$: Similar to f_0, we have $|A^g| = 4^6$.
- $g = f_1$: We have four choices of colour for each of the sides B, C, D, E and F. Side A must be the same as B, J must be the same as C, I must be the same as D, H must be the same as E and G must be the same as F. So in total we have 4^5 colourings that are fixed by f_1.
- $g = f_3, f_5, f_7, f_9$: Similar to f_1, we have $|A^g| = 4^5$.
- $g = r$: Each side must be the same as the side adjacent to it, so every side must have the same colour. We have 4 colourings that are fixed by r.
- $g = r^2$: every second side must have the same colour. We have 4 choices of colour for side A, and then we must use that colour for C, E, G and I. We also have 4 choices of colour for side B, and then we must use that colour for D, F, H and J. In total we have 4^2 colourings that are fixed by r^2.
- $g = r^3$: Every third side must be the same colour, but notice that if we colour side A and then go counterclockwise around the bracelet colouring every third side that same colour, we end up colouring every side (this is because $\gcd(3, 10) = 1$). So in fact all sides have the same colour, and there are a total of 4 colourings of the bracelet that are fixed by r^3.
- $g = r^4, r^6, r^8$: For r^4, every fourth side must be the same colour, but if we colour side A and then go counterclockwise around the bracelet colouring every fourth side that same colour, we end up colouring every second side. So in fact we colour A, C, E, G, and I the same colour,and we colour B, D, F, H and J the same colour. This means there are 4^2 colourings that are fixed by r^4. The situation for r^6 and r^8 are the same.
- $g = r^5$. Every fifth side must have the same colour. So we have four choices of colour for eaech of the sides A, B, C, D and E, and then each of the sides F, G, H, I and J must be the same colour as the side opposite it. This means there are 4^5 colourings that are fixed by r^5.
- $g = r^7, r^9$. Similar to r^3, since 7 and 9 are also relatively prime with 10. We have $|A^g| = 4$.

We summarize the results in the table below:

$g \in G$	$\lvert A^g \rvert$
e	4^{10}
f_0, f_2, f_4, f_6, f_8	4^6
f_1, f_3, f_5, f_7, f_9	4^5
r, r^3, r^7, r^9	4
r^2, r^4, r^6, r^8	4^2
r^5	4^5

Therefore by Burnside's Lemma, the number of inequivalent colourings of the bracelet (ie. arrangements of beads) is

$$
\begin{aligned}
|A/D_{10}| &= \tfrac{1}{|D_{10}|} \sum_{g \in D_{10}} |A^g| \\
&= \tfrac{1}{20} \left(4^{10} + 5(4^6) + 5(4^5) + 4(4) + 4(4^2) + 4^5\right) \\
&= 53746.
\end{aligned}
$$

4. Let G, H, and K be groups and let $\phi : G \to H$ and $\psi : H \to K$ be isomorphisms.
   (a) Show that ϕ^{-1} and $\psi \circ \phi$ are both isomorphisms. (The first part of this amounts to proving Theorem 3.12.3.)
   (b) Using (a), show that the isomorphism of groups determines an equivalence relation on the set of all groups. That is, show that $\cong$ is an equivalence relation on the set of all groups.

Solution:

(a) It is clear that $\phi^{-1} : H \to G$ exists since ϕ is by definition a bijection. Moreover, since ϕ^{-1} has an inverse function (namely ϕ), it is a bijection. Now we only need to prove that ϕ^{-1} is a homomorphism.

Let x and y be any elements of H. Since ϕ is onto, there exist a and b in G such that $x = \phi(a)$ and $y = \phi(b)$. Then

$$
\begin{aligned}
\phi^{-1}(xy) &= \phi^{-1}(\,\phi(a)\,\phi(b)\,) \\
&= \phi^{-1}(\,\phi(ab)\,) && \text{since } \phi \text{ is an isomorphism} \\
&= ab \\
&= \phi^{-1}(\,\phi(a)\,)\,\phi^{-1}(\,\phi(b)\,) \\
&= \phi^{-1}(x)\,\phi^{-1}(y).
\end{aligned}
$$

This shows that ϕ^{-1} is an isomorphism.

Now we show that $\psi \circ \phi$ is an isomorphism. Once again, since ϕ and ϕ are isomorphims, we know they are bijections and therefore they have inverses, ϕ^{-1} and ψ^{-1}. The function $\psi \circ \phi : G \to K$ has inverse $\phi^{-1} \circ \phi^{-1}$, and therefore it is a bijection. Now all that remains is to show that $\psi \circ \phi$ is a homomorphim.

Let a and b be any elements of G. Then

$$
\begin{aligned}
(\psi \circ \phi)(ab) &= \psi(\,\phi(ab)\,) \\
&= \psi(\,\phi(a)\,\phi(b)\,) && \text{since } \phi \text{ is a homomorphim} \\
&= \psi(\,\phi(a)\,)\,\psi(\,\phi(b)\,) && \text{since } \psi \text{ is a homomorphism} \\
&= (\psi \circ \phi)(a)\,(\psi \circ \phi)(b),
\end{aligned}
$$

as required.

(b) To see that isomorphism is reflexive, note that for any group G, the identity function $\varepsilon_G : G \to G$, defined by $\varepsilon_G(g) = g$ for all $g \in G$, is an isomorphism. This means that $G \cong G$. Now let G and H be two groups such that $G \cong H$. Then there exists an isomorphims $\phi : G \to H$. Since the function $\phi^{-1} : H \to G$ is also an isomorphism, by part (a), we have $H \cong G$. So isomorphism is a symmetric relation. Finally, suppose $G \cong H$ and $H \cong K$, for groups G, H and K. Then there is an isomorphims $\phi : G \to H$ and an isomorphim $\psi : H \to K$. By (a), the function $\psi \circ \phi : G \to K$ is an isomorphism, so $G \cong K$. Therefore isomorphism is a transitive relation. It follows that isomorphism is an equivalence relation.

5. Let G and H be groups and let $f : G \to H$ be an isomorphism. Prove that G is abelian if and only if H is abelian. (This is part 7 of Theorem 3.12.2.)

Solution: First, suppose that G is abelian. We show H is. Let h_1 and h_2 be two elements of H. As f is a surjection, we can find g_1 and g_2 in G with $f(g_1) = h_1$ and $f(g_2) = h_2$. Then we have

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1,$$

where we have used the fact that G is abelian in the third equality and the fact that f is an isomorphism in the second and fourth.

Conversely, suppose that H is abelian. Let g_1 and g_2 be two elements of G. We have

$$f(g_1g_2) = f(g_1)f(g_2) = f(g_2)f(g_1) = f(g_2g_1)$$

where we have used the fact that H is abelian in the second equality and the fact that f is an isomorphism in the first and third. Now, since f is injective, we have $g_1g_2 = g_2g_1$. As g_1, g_2 were arbitrary, G is abelian.

6. Let G be the set of matrices of the form

$$\begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix},$$

where $j \in \{0, 1\}$ and all entries of the matrix are elements of $\mathbb{Z}_n$ (so all operations on the entries are done modulo n); that is, the entries of the matrix are really $[-1]_n^j$, $[k]_n$, $[0]_n$ and $[1]_n$. With matrix multiplication, G is a group (you do not need to prove this). Prove that G is isomorphic to D_n by finding an explicit isomorphism (and proving that it is an isomorphism).

Solution:

We define the function $f : G \to D_n$ by

$$f\left(\begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix}\right) = r^k h^j.$$

Since $r^n = e$ in D_n, we have $r^k = r^\ell$ for integers k and ℓ if and only if $k \equiv \ell \bmod n$. In other words, $r^k = r^\ell$ if and only if $[k]_n = [\ell]_n$, so our function f is well-defined.

An arbitrary element of D_n can be written as $r^k h^j$, where $j = 0$ or 1 and $0 \leq k \leq n-1$. We see that $r^k h^j = f\left(\begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix}\right)$, so f is onto. Now, since there are 2 distinct values allowed in the $(1,1)$-entry of a matrix $\begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix}$, and n distinct equivalence classes allowed in the $(1,2)$- entry, there are a total of $2n$ elements of G. Since G and D_n have the same cardinality, it follows that f is not only onto but also one-to-one. So f is a bijection.

Recall that in D_n, we have the relation

$$hr^i = r^{n-i}h = r^{-i}h,$$

so

$$h^2 r^i = hhr^i = hr^{-i}h = r^{-(-i)}hh = r^i h^2,$$

and

$$h^3 r^i = hhhr^i = hhr^{-i}h = hr^i hh = r^{-i}hhh = r^{-i}h^3,$$

and so on. We see a pattern:

$$h^j r^i = r^{(-1)^j i} h^j. \tag{1}$$

This will be helpful in showing that f is a homomorphism.

Let $g = \begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix}$ and $h = \begin{bmatrix} (-1)^i & \ell \\ 0 & 1 \end{bmatrix}$ be any elements of G. Then

$$\begin{aligned}
f(g)f(h) &= f\left(\begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix}\right) f\left(\begin{bmatrix} (-1)^i & \ell \\ 0 & 1 \end{bmatrix}\right) \\
&= (r^k h^j)(r^\ell h^i) \\
&= r^k (h^j r^\ell) h^i \\
&= r^k (r^{(-1)^j \ell} h^j) h^i \qquad \text{by (1)} \\
&= r^{k+(-1)^j \ell} h^{i+j} \\
&= f\left(\begin{bmatrix} (-1)^{i+j} & k+(-1)^j \ell \\ 0 & 1 \end{bmatrix}\right) \\
&= f\left(\begin{bmatrix} (-1)^j & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} (-1)^i & \ell \\ 0 & 1 \end{bmatrix}\right) \\
&= f(gh).
\end{aligned}$$

Therefore f is a homomorphism. Since it is also a bijection, it follows that it is an isomorphism. Therefore $G \cong D_n$.

7. Which of the following groups are isomorphic?

- $\mathbb{Z}$ (with addition)
- The subgroup $\langle r^6 \rangle$ of D_8 (with composition)
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (with componentwise addition)
- $8\mathbb{Z} = \{\dots, -16, -8, 0, 8, 16, \dots\}$ (with addition)
- $\mathbb{Z}_4$ (with addition)
- $G = \{f_n | n \in \mathbb{Z}\}$, where f_n is the function on $\mathbb{Z}$ defined by $f_n(x) = n + x$ for all $x \in \mathbb{Z}$ (with composition)
- U_5 (with multiplication)
- U_8 (with multiplication)

By problem 4(b), $\cong$ is an equivalence relation on the set of all groups, so this question amounts to sorting the above groups into their equivalence classes. Each time you add a new group to an equivalence class, give a specific isomorphism from that group to one of the groups already in the equivalence class. (You must be sure that your function actually is an isomorphism, but you do not need to include the proof in your answer.) Each time you add a new equivalence class to your list, give a reason why the groups in the new class do not belong in any of the equivalence classes you have already listed.

Solution:

- $\{\mathbb{Z}, 8\mathbb{Z}, G\}$ is one equivalence class. To see that $8\mathbb{Z} \cong \mathbb{Z}$, note that the fuction $\phi : \mathbb{Z} \to 8\mathbb{Z}$ defined by $\phi(x) = 8x$ for all $x \in \mathbb{Z}$ is an isomorphism. To see that $G \cong \mathbb{Z}$, note that the function $\phi : \mathbb{Z} \to G$ defined by $\phi(x) = f_x$ is an isomorphism.
- Since all the other groups are finite, they cannot be in the same equivalence class as $\mathbb{Z}$. We need another equivalence class. Let's find the equivalence class of $\mathbb{Z}_4$ first. It is $\{\mathbb{Z}_4, U_5\}$. Since U_5 is a cyclic group of order 4, Theorem 3.12.4 guarantees that $U_5 \cong \mathbb{Z}_4$. To find an explicit isomorphism from $\mathbb{Z}_4$ to U_5, we note that U_5 has generator $[2]_5$ and $\mathbb{Z}_4$ has generator $[1]_4$. For each element $i[1]_4 \in \mathbb{Z}_4$, we define $\phi(i[1]_4) = {[2]_5}^i$. This is an isomorphism.
- To see that U_8 is not in the same equivalence class as $\mathbb{Z}_4$, we note that U_8 is not cyclic (and the same is true of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$). However, these two groups are isomorphic to each other; that is, the final equivalence class is $\{U_8, \mathbb{Z}_2 \oplus \mathbb{Z}_2\}$. Define $\phi : U_8 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by $\phi([1]_8) = (0, 0)$, $\phi([3]_8) = (0, 1)$, $\phi([5]_8) = (1, 0)$, $\phi([7]_8) = (1, 1)$.

  It is not necessary (for the assignment problem) to prove that this ϕ is an isomorphism, but here is an example of how to do that.

  Clearly ϕ is a bijection. To see that ϕ preserves operation, we will construct operation tables.

  The operation table for U_8 (writing 3 instead of $[3]_8$, etc.) is

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

  Applying ϕ to each entry in the above table gives

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$,

  and this is exactly the same as the operation table for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. This shows that ϕ preserves operation.

You may be wondering how this constitutes a proof. Here's how:

By constructing the table for U_8 and then applying ϕ to each element of the table, we have computed ab and then $\phi(ab)$ for every $a, b \in U_8$.

On the other hand, imagine we start with the table

$\cdot$	1	3	5	7
1				
3				
5				
7				

and the we apply ϕ to the elements of U_8 individually:

$+$	$\phi(1)$	$\phi(3)$	$\phi(5)$	$\phi(7)$
$\phi(1)$				
$\phi(3)$				
$\phi(5)$				
$\phi(7)$				

becomes

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$				
$(0,1)$				
$(1,0)$				
$(1,1)$				

We have now computed $\phi(a)$ and $\phi(b)$ for all $a, b \in U_8$. When we fill in the rest of the entries of this operation table (that is, when we complete the operation table for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$), we are computing $\phi(a) + \phi(b)$ for all $a, b \in U_8$. That is, the second table represents *simultaneously* the result of

- computing ab for all $a, b \in U_8$ and then computing $\phi(ab)$, *and*
- computing $\phi(a)$ and $\phi(b)$ for each $a, b \in U_8$ and then computing $\phi(a) + \phi(b)$.

This tells us that $\phi(ab) = \phi(a) + \phi(b)$ for all $a, b \in U_8$.

8. Let $\mathbb{R}^\times$ be the set of nonzero real numbers with multiplication. Following the proof of Cayley's Theorem, $\mathbb{R}^\times$ is isomorphic to the subgroup $H = \{f_g \mid g \in \mathbb{R}^\times\}$ of $S_{\mathbb{R}^\times}$.

   (a) Describe the element f_{10} of H, and the inverse of this element.

   (b) Find an element of $S_{\mathbb{R}^\times}$ which is not in H.

   (c) Without using your answer from (b), give another reason why H cannot be all of $S_{\mathbb{R}^\times}$. (If it is, then $S_{\mathbb{R}^\times}$ is isomorphic to $\mathbb{R}^\times$. Using group properties, explain why this cannot be the case.)

Solution:

(a) The function $f_{10} : \mathbb{R}^\times \to \mathbb{R}^\times$ is defined by $f_{10}(x) = 10x$ for all $x \in \mathbb{R}^\times$. The inverse of f_{10} is $f_{0.1} : \mathbb{R}^\times \to \mathbb{R}^\times$ defined by $f_{0.1}(x) = 0.1x$ for all $x in \mathbb{R}^\times$. To verify that it is the inverse, we confirm that for any $x \in \mathbb{R}^\times$,

$$f_{10} \circ f_{0.1}(x) = f_{10}(f_{0.1}(x)) = f_{10}(0.1x) = 10(0.1x) = x,$$

so $f_{10} \circ f_{0.1} = I_{\mathbb{R}^\times}$, the identity function on $\mathbb{R}^\times$. In a similar way we can show that

$$f_{0.1} \circ f_{10} = I_{\mathbb{R}^\times},$$

and so $f_{0.1}$, as defined above, is the inverse of f_{10}.

(b) Let $h : \mathbb{R}^\times \to \mathbb{R}^\times$ be the function defined by $g(x) = \frac{1}{x}$, for all $x \in \mathbb{R}^\times$. This function is a bijection on $\mathbb{R}^\times$, so it is in $S_{\mathbb{R}^\times}$ but it is not equal to f_g for any $g \in \mathbb{R}^\times$ because there is no $g \in \mathbb{R}^\times$ for which $gx = \frac{1}{x}$ for all $x \in \mathbb{R}^\times$.

(c) As noted, if H were all of $S_{\mathbb{R}^\times}$, then Cayley's Theorem would imply that $\mathbb{R}^\times \cong S_{\mathbb{R}^\times}$. However, this cannot be the case because $\mathbb{R}_\times$ is an abelian group and $S_{\mathbb{R}^\times}$ is non-abelian.